A Case for Implementation of Citizen Centric National Identity Management Systems

Crafting a Trusted National Identity Management Policy

Adjei, Joseph K.

A Case for Implementation of Citizen Centric National Identity Management Systems:

Crafting a Trusted National Identity Management Policy

A Thesis Submitted in Partial Fulfillment of the Requirement for the Degree of Doctor of Philosophy

Revised version, October 2013

Joseph Kwame Adjei

Center for Communication, Media and Information Technologies (CMI)

Aalborg University Copenhagen, Denmark

AALBORG UNIVERSITY
DENMARK

Mandatory Page

Thesis Title: **A Case for Implementation of Citizen Centric National Identity Management Systems; Crafting a Trusted National Identity Management Policy**

Supervisor: Henning Olesen (Associate Professor)

List of published papers:

Paper I: Adjei & Tobbin, (2011) Identification Systems in Africa; The Case of Ghana Published in proceedings of the 12th International Symposium on Information Science (ISI 2011), 9 - 11 March 2011, Hildesheim. (Internationales Symposium für Informationswissenschaft, Hildesheim, 9.—11. März 2011)

Paper II Adjei & Olesen, (2011) Analysis of Privacy-Enhancing Identity Management Systems. A paper published in the Proceedings of WRF26-WG1, Doha, Qatar.

Paper III Adjei & Olesen, (2011) Keeping Identity Private; Establishing Trust in the Physical and Digital World for Identity Management Systems Published in IEEE Vehicular Technology Magazine September 2011

Paper IV Adjei & Olesen, (2012) Secondary Uses of Personal Identity Information: Policies, Technologies and Regulatory Framework Published in Digiworld Economic Journal, no. 88, 4th Q. 2012, p. 79.

Paper V Adjei & Olesen, (2012) Building Trusted National Identity Management Systems – Presenting Privacy-Concern Trust Model. CENTRIC 2012, Proceedings of The Fifth International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, pp 19-26; November 18-23, 2012 - Lisbon, Portugal

Paper VI Joseph K. Adjei, (2013) Towards a Trusted National Identities Framework Published in Emerald, Info Volume 15, Issue (1), pp 48-60.

This thesis has been submitted for assessment in partial fulfillment of the PhD degree. The thesis is based on the submitted or published scientific papers which are listed above. Parts of the papers are used directly or indirectly in the extended summary of the thesis. As part of the assessment, co-author statements have been made available to the assessment committee and are also available at the Faculty. The thesis is not in its present form acceptable for open publication but only in limited and closed circulation as copyright may not be ensured.

Acknowledgements

Taking a reflective view of all the happenings leading to the successful completion of my thesis, i cannot, but stand in awe. It is from this context that I thank God for His abundant grace and mercy, and endowing me with sufficient grace, good health, financial support and understanding which have sustained me and my family throughout this challenging period. For this cause, I will bless the Lord at all times and His praise shall continually be in my mouth.

I wish to share the credit of my work with all the people who have helped me, in different ways, during my PhD study. First of all, I would like to sincerely thank Associate Professor Henning Olesen, my supervisor, for his invaluable contribution to my scientific research and for all the opportunities he gave me during these last three years, and also for the constant presence, guidance, and advice. His leadership, support, attention to details and insightful comments is an example I would emulate. I also like to express my sincere gratitude to Professor Knud Erik Skouby for his leadership, Dr Gamel Wiredu for his lecture on academic research, and Dr Edgar Whitley for his constructive critique of my study plan and some of my publications. I am indebted to Anette Bysoe, and the wonderful CMI team of Professors and researchers, for always being there to provide support when I needed it and for cheering me on. I would like to thank Dr. Peter Tobbin and my other PhD colleagues, for their invaluable critique of different phases of my PhD studies. I would like to thank Abena Offe and the late Florence Onny who assisted me during the organisation of the two stakeholder workshops and focus group discussions. I would like to thank Divine and Rebecca of Brookes Institute for their assistance in organising the interviews, fora, workshops and logistics during these years. Last but not the least, my family, especially my wife Veronica, my late mother who could not live long enough to see the end of this project, my fathers Mr Kwabena Adjei and Bishop Ishmael Sam, and my three daughters; Eirene, Angela and Joan-Danielle, deserve all my gratitude for giving me the opportunity to undertake this project in the first place, always supporting me over three years, and for always being there. I am forever grateful to you all.

Abstract

Technological advancements have paved the way for fast, easy and relatively cheap collection, aggregation and analysis of large volumes of data by organisations, with little or sometimes, no human interventions. Such technological advancements have also made it increasingly possible for organisations to; electronically establish the social connections of many people, provide location independent services and seamless flow of information. The World Economic Forum has even projected that by the year 2015, about 1 trillion devices will be connected to the Internet worldwide. Such a phenomenal development is given credence by effective exchanges of personal identity information, since many commercial transactions and social interactions require some degree of personal information disclosure. Thus, personal identity information has become an integral part of modern business models.

However, the risk of not realizing such value of personal information is evident in many instances, given the height of societal concerns about security and privacy, and the diminishing level of trust in transacting parties. Such societal concerns also have governance implications in many countries. Policy makers therefore try to implement identity policies with the view of curtailing identity abuses, promote the seamless flow of business transactions, and to provide citizens the ability to exercise informational self-determination. Identity policies are usually also associated with implementation of identity management systems.

Previously, the design of such systems has largely focused on stringent security requirements with minimal attention focus on citizens and their concerns (citizen-centric). Various identity related research initiatives have thus, been carried out in OECD member countries, aimed at designing and developing identity management systems that is user centric and privacy enhancing.

Many of the proposed privacy enhancing solutions implicitly assume availability of internet connectivity, user awareness and exposure, and high level of literacy. Ironically, developing countries are characterised by many infrastructural challenges, low literacy level and thus, hampering effective uses of identity management systems. Moreover, implementation of such systems unduly emphasize on silo identity management systems and on physical verification of credentials with its propensity to limit the benefits that can be derived from such investments.

This PhD study adapts the Delone and Mclean's IS success model to analyse the factors that affect effective uses of national identity management systems, using a qualitative case study research approach. Empirical data were gathered in Ghana through a combination of quasi

statistical survey and problem structuring methodology. The choice of Ghana as case country was due to the fact that the dynamics typify the identification challenges in many developing countries. The study has shown that effective uses of identity management systems depend on efficient civil registration systems, user involvement and institutional cooperation. It has also shown that, for effective uses of identity management systems, policy makers must ensure the attainment of the threshold level of trust. This is the level where privacy concern is low and trust is high enough to encourage institutional cooperation and secondary uses of personal information.

The study contributes to the identity management literature by enriching our current understanding of the key factors that are essential for the successful implementation of national identity management systems, and also provides guidelines for developers and policy makers for establishing future ecosystem of trusted identities.

Resume

Teknologiske fremskridt har banet vejen for, at organisationer hurtigt, nemt og relativt billigt kan indsamle, aggregere og analysere store datamængder, ofte uden menneskelig medvirken. Sådanne teknologiske fremskridt har også i stigende grad gjort det muligt elektronisk at etablere omfattende sociale netværk, levere lokationsuafhængige tjenester og muliggøre uhindret informationsudveksling. World Economic Forum forudsiger, at omkring 1 billion enheder vil være forbundet til Internettet på verdensplan i 2015. En så fænomenal udvikling vil bl.a. kræve en effektiv udveksling af personlig identitetsinformation, fordi mange kommercielle transaktioner og sociale interaktioner indebærer, at der frigives personlig information. Personlige oplysninger er således blevet en integreret del af moderne forretningsmodeller.

Men risikoen for ikke at udnytte værdien af personlige oplysninger er åbenbar, set i lyset af de samfundsmæssige betænkeligheder omkring sikkerhed og privatlivets fred og den manglende tillid mellem de involverede parter ved transaktioner på Internettet. Sådanne samfundsmæssige hensyn har også reguleringsmæssige konsekvenser i mange lande. Politikerne må derfor forsøge at indføre regler for håndtering af identiteter med henblik på at begrænse identitetsmisbrug, fjerne hindringer for forretningstransaktioner og give borgerne mulighed for at udøve kontrol og selvbestemmelse over deres data.

Sådanne identitetspolitikker er som regel også knyttet til implementering af identity management-systemer. Tidligere har design af sådanne systemer i vid udstrækning fokuseret på de strenge sikkerhedskrav og kun i ringe omfang på borgerne og deres bekymringer, hvad angår personlige data. Et antal identitetsrelaterede forskningsinitiativer er derfor blevet gennemført i forskellige OECD-lande med henblik på at designe og udvikle identity management-systemer, der er mere brugercentrerede og privatlivsfremmende.

Desværre bygger mange af de foreslåede løsninger til beskyttelse af persondata på implicitte antagelser om tilgængeligheden af internet-adgang, brugernes bevågenhed og et højt niveau af læsefærdigheder. Ironisk nok er udviklingslande præget af manglende infrastruktur og analfabetisme, og dette vanskeliggør effektive anvendelser af identity management-systemer. Endvidere har den hidtidige implementering af sådanne systemer haft karakter af "siloer" med fokus på fysisk verifikation af identitetsbeviser, hvilket har ført til begrænsninger af de fordele, der kan opnås.

I dette ph.d.-projekt anvendes og udbygges Delone og McLean's succesmodel for informationssystemer til at analysere de faktorer, der er væsentlige for en effektiv anvendelse af nationale identity management-systemer med en kvalitativ case study-orienteret forskningstilgang. De empiriske data blev indsamlet i Ghana gennem en kombination af quasi-statistisk under-

søgelse og problemstruktureret metodik. Valget af Ghana som case understøttes af, at de identifikationsmæssige problemer og udfordringer kan anses som værende typiske for mange udviklingslande. Projektet har vist, at effektiv anvendelse af identity management-systemer er afhængig af velfungerende cpr-systemer, brugerinddragelse og samarbejde på tværs af institutioner. Det har også vist, at for at sikre en sådan effektiv anvendelse må de politiske beslutningstagere først etablere de fornødne rammer for, at tilliden mellem de involverede parter kan være til stede. Der kræves et vist tærskelniveau, hvor bekymringen om beskyttelse af privatlivet er tilstrækkeligt lav, og tilliden er tilstrækkeligt høj til at fremme institutionelt samarbejde og sekundære anvendelser af personlige oplysninger, f.eks. til kommercielt brug.

Projektet bidrager til identity management-litteraturen med en øget forståelse af de nøglefaktorer, der er væsentlige for en vellykket implementering af nationale identity management-systemer og med anbefalinger til udviklere og politikere om etablering af et fremtidigt økosystem for trusted identities.

Table of Contents

List of Figures

List of Tables

Abbreviations and Acronyms

AFIS	Automated Fingerprint Identification System
ECOWAS	Economic Community of West African Countries
HDI	Human Development Index
ICT	Information and Communication Technology
IdM or IDM	Identity Management
IdMS or IDMS	Identity Management Systems
IS	Information Systems
OECD	Organisation for Economic Cooperation and Development
TAM	Technology Acceptance Model
TIN	Tax Identification Numbers
UNDP	United Nations Development Programme
UNICEF	United Nations Children's Fund
UTAUT	Unified Theory of Acceptance and Use of Technology
NIdMS or NIDMS	National Identity Management Systems
CPR	Centrale Person Register
NIA	National Identification Authority
GRA	Ghana Revenue Authority
DVLA	Driver and Vehicle Licensing Authority
CRS	Civil Registration System
NFC	Near field communication
RFID	Radio Frequency Identification

Chapter 1: Introduction

This chapter provides an overview of the research conducted during the entire PhD project spanning February 2010 to January 2013. It begins with an initial observation of the research gap in trusted identity management system (IDMS). Subsequently, it continues logically with a presentation of the theoretical rationale of the study by touching on the need for guidelines for trusted national identities policy formulation, within the context of developing countries[1]. This background provides the basis for specifying the phenomenon of interest, defining the research questions and objectives, and the positioning of the research within the domain of identity management. A summary of the philosophical paradigm, research methodology and findings are then presented. The chapter concludes with an outline of the structure of the thesis.

1.1 Background & Purpose

The overarching purpose of this research effort is to examine the ensuing phenomenon when government agencies implement identity management systems with the aim of enabling effective interactions, identity verification, provision of access to government services, and to facilitate electronic commerce transactions, particularly "secondary uses[2]" of personal identity information[3].

Technological advancements have paved the way for fast, easy and relatively cheap collection, aggregation and analysis of large volumes of data by organizations, with little or sometimes, no involvement of the originator and/or the data subject[4] (France Bélanger & Crossler, 2011; Malhotra, Kim, & Agarwal, 2004). Presently there are about 6 billion mobile phone subscriptions in the world, and on a daily basis, 10 billion text messages are exchanged, and 1 billion entries are posted on blogs or social networks worldwide (World Economic Forum, 2012a). It is even becoming increasingly possible to see the social connections of many peo-

[1] A developing country is a country with relatively low standard of living, undeveloped industrial base, moderate to low Human Development Index relative to other countries and dependent on low value added sectors, e.g. agriculture, mining, etc. For the purpose of this study countries in the lower middle income group are also regarded as developing countries.

[2] Secondary use of personal information is the collection and storage of information for purposes other than originally intended, whether legitimate or otherwise.

[3] See section 2.4. Privacy and Personal identity information for detailed explaination

[4] Data subject is an individual to whom personal data relates.

ple on the Internet. Intertwined with such staggering technological advancement is also the increasing relevance of cloud computing with its unique characteristics of on-demand self-service, resource pooling that is independent of location, ubiquitous network access, flexibility, and thoughtful service, all of which are geared toward a seamless flow of information and transactions. In fact, it is estimated that by 2015, 1 trillion devices will be connected to the Internet worldwide (World Economic Forum, 2012a).

At the core of these phenomenal developments is the commoditisation[5] of personal identity information, which has become a key component of modern business models. Thus, the effective use of personal information can drive innovation, investment and sustainable economic growth, and greatly improve social security and security services (World Economic Forum, 2012a).

However, the risk of not realizing such value of personal information is evident given the height of societal concerns about security and privacy, and the diminishing level of trust between transacting parties. Yet parties in business transactions and social interactions usually rely on the issue of claims, and disclosure of unique attributes and credentials[6] for proofs of identity. Governments in many countries have responded to the challenge and the uncertainties by implementing various forms of electronic identity management systems as a critical enabler of government to citizens' interactions, facilitating business transactions and citizens' access to social services (J. K. Adjei, 2012).

Ironically, implementation of IDMS and adoption by citizens usually present complex issues, for the key stakeholders, given that identity policies usually transcend technological, security, institutional, and economic barriers and also borders on issues of information privacy and trust (J. K. Adjei & Olesen, 2012). The complexity is often compounded by the rate at which standards and technological solutions become obsolete; and the increased link-ability of information to the data subject, with its tendency to raise privacy concerns (M. Culnan, 1993). Governments therefore find it difficult to justify such investments, and thus often leads to discomfort (Seltsikas & O'Keefe, 2010; E. A. Whitley & Hosein, 2010). Thus the concept of privacy, user-centricity, trusted identities and identity assurance have taken centre-stage in the IDMS discussions, even beyond the architectural issues like identity federation and silos

[5] Commoditisation is used interchangeably with commodification to describe the process of making commodities out of any thing that did not used to be available for trade previously

[6]Credential is a generic term that can apply to both paper documents like Passports or Birth Certificates, and non-paper based objects such as smartcards and other tokens.

(Camenisch et al., 2011; Crosby, 2008a; Evry, 2010; Grant, 2011a; E. Whitley & Kanellopoulou, 2010a). Various privacy enhancing IDMSs are being piloted in many OECD[7] countries (Camenisch, 2012; IBM, 2010; Microsoft, 2011).

In developing countries, identification challenges continue to persist, although various forms of credentials and tokens have been issued to citizens. There is also an undue emphasis on physical verification of credentials, with many of the IDMS being in silos, yet many of the structural identification challenges persist. In Ghana, for instance, several different IDMS have been implemented leading to the issue of various forms of credentials. National Identification Cards, Birth Certificates, National Health Insurance Cards, Biometric Passports, Biometric Driver's Licenses, Biometric Voter's Identity Cards and Tax Identification Numbers (TIN) are some of the widely used credentials and identifiers[8]. Many of the source documents required for the issue of credentials are usually unreliable and takes longer time to verify. For example the civil registration coverage is currently 71% according to UNICEF 2012 statistics (UNICEF, 2012), implying that birth certificates could not be the only reliable source document for acquisition of identity credentials. This situation hinders the reliability of identity credentials and tokens for proofs of identity and for secondary uses by businesses and government agencies.

Existing IDMSs are primarily used by the credential issuers or (identity providers)[9] as a means of fulfilling their primary functions – e.g. voters' identity card is for electoral purposes. Changes to citizens personal data (addresses, etc.) are handled by each of the credential issuers separately resulting in various errors and data and effort duplications. Moreover, Internet applications of IDMS are not given the requisite attention and thus identification systems typically focus on physical credential examination that cannot be verified electronically by the other institutions that depend on it. Thus, service providers have no legal process of verifying and authenticating credentials in real-time, resulting in each service provider devising their own specific means of identity verification. In spite of its use being lower than expected,

[7] The Organisation for Economic Co-operation and Development (OECD) is currently made up of 34 countries including European Union member countries, Australia, Canada, Chile, Japan, Korea, Israel, Mezico, New Zealand, Turkey and USA.

[8] An identifier is a name that identifies or labels the identity of a person or entity. An identifier may be a word, number, letter, symbol, or any combination of those.

[9] Credential issuers or (identity providers) are institutions that issue credentials which can be used for proofs of identity.

identity management can play a central role, if the factors that affect its takeoff are properly addressed as it is evidenced in recent statistics in Europe (TNS Opinion & Social, 2011). For instance a recent euro-barometer survey revealed that 62% of users better understand how to protect their identity in offline transactions using data minimization techniques, whilst 86% trust public institutions and 73% banks (TNS Opinion & Social, 2011).

Contrarily, the 2012 global information technology report (Dutta & Bilbao-Osorio, 2012) rated Ghana and many African countries at the lowest in all the indices. Ghana was ranked 97th out of the 142 countries covered whilst the top 20 positions were all occupied by either European or OECD countries. In the United States, trusted identities ecosystems have been found to be very critical to the success of digital IdMS (Grant, 2011a). This study focuses on understanding the stakeholder concerns on identity management and offering design guidelines for developers and policy makers in crafting trusted identity management systems that ensure citizens' trust and information privacy regarding the collection, storage, use, and dissemination of personal identity information (Bennett & Raab, 2003a).

1.2 Theoretical Rationale of the Study

> "How can a person just DECIDE what he's going to think? Doesn't he have to think FIRST, and then try to discover what it is that he's THOUGHT?"
>
> - Lucy and Linus, "Peanuts" by Charles Schulz, April 1961[10]

The central theme of this study is positioned within the Information Systems (IS) broad subject. Thus, a digital identity management system is a type of information system whereas citizen-centric digital identity management falls within the broad theme of digital identity management systems as depicted in Figure 1.

Since DeLone and McLean developed their seminal paper, IS Success model in 1992, several studies on IS success or effectiveness have ensued in the past twenty years. A preliminary analysis of IS success studies by juxtaposing IDMS studies revealed a paucity of literature on the key factors that influence the success or effectiveness of national identity management system (NIDMS). Even more pronounced were IS success studies that deal with stakeholder involvement, or with privacy and trust issue. Moreover, research has mainly focused on assessing success from either organizational or user perspectives (Petter, DeLone, & McLean,

[10] Charles Monroe Schulz (November 26, 1922 – February 12, 2000) was an American cartoonist, best known for the comic strip Peanuts.

2012). Since NIDMS has societal implications, its success must be measured by taking into consideration, the impact on society.

Ironically, in their recent study on the past, present and the future IS of success, Petter et al., (2012) posited that "in the current generation of systems and in future eras, we must go beyond the undue focus on developers, users, and managers and find other key stakeholders, including customers, employees, suppliers, stockholders, vendors, and governments" (Petter et al., 2012). Such calls sum up the need for IS success study that takes a multi-stakeholder perspective.

Secondly, existing IDMS research discourse revolves around IDMS technologies, and design and solutions that claim to address minimum disclosure issues like touch2id, U-prove, idemix, etc. (Evry, 2010; IBM, 2010; Microsoft, 2011; Recordon & Reed, 2006) and also address the fine-grained concerns of stakeholders. Digital identity management must however strike a balance between usability, security, and privacy (Bertino, Paci, Ferrini, & Shang, 2009; Bertino & Takahashi, 2010; Rahaman & Sasse, 2010), For instance, *how to make personal identification information available, only to the appropriate individuals or services*; *how to build trust between parties involved in identity transactions;* and *how to reduce the abuse of personal identity information* (Baldwin, Casassa Mont, Beres, & Shiu, 2010). Such a condition requires clear understanding of the consequences of lack of trust.

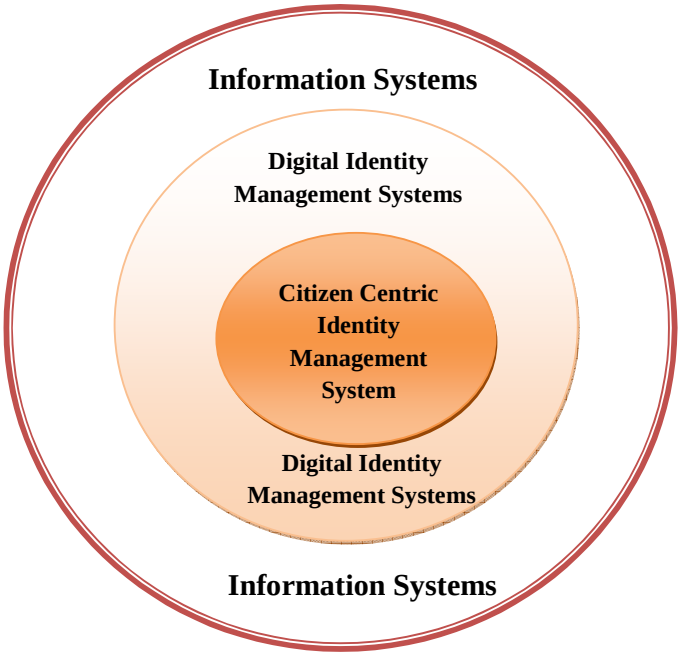


Figure 1 Research Focus.

In particular, factors that contribute to lack of trust in national IDMS and the relationship between trust and citizens' concerns regarding secondary uses of personal identity information.

How to build trusting relationships within the identity ecosystem are major concerns that research must address. Lack of trust or otherwise does not exclusively originate from technological factors but rather many of such factors might be shrouded in contextual colours. A critical analysis of trusted identity management systems literature manifested the need for guidelines on its effective uses, especially from developing countries' perspectives, given that much of the existing research and initiatives fails to anticipate the contextual issues in such an important constituency.

There is therefore the need to draw from information systems success literature to find answers to such questions. DeLone & McLean's IS success model (Delone & McLean, 2003; DeLone & McLean, 1992; Petter, DeLone, & McLean, 2008; Petter et al., 2012), technology acceptance model (TAM) (F. D. Davis, 1989) and user involvement theory (B. Ives & Olson, 1984) could be beneficial lenses for addressing user concern in order to ensure effectiveness of identity management systems. In particular the IS success model is used in accessing the overall benefits that can be derived from the implementation of IS. Although several variations of it have been introduced (V. Venkatesh, Morris, Davis, & Davis, 2003), TAM has been predominantly used to explain consumer behavior with respect to technology acceptance and user satisfaction. IS success model also ensure consistency in success measures and the clarification of an important dependent variable in IS success research (Delone & McLean, 2003; DeLone & McLean, 1992; Petter et al., 2008).

Additionally, many innovative privacy enhancing IDMS technological initiatives assume a certain baseline of user awareness and literacy. However, the high illiteracy level in many developing countries is obvious, as Figure 2 indicates. In Ghana for instance, the literacy percentage from age fifteen (15) upwards is on average 67% based on the most recent UNESCO report as shown in Figure 2 (UNESCO, 2010). Clearly, this implies that 33% of the population are illiterate. Thus the relevance of privacy enhancing principles and guidelines that seeks to give users control over their personal information use, minimal data disclosure, and justifiable consent (K. Cameron & Jones, 2007; OECD, 1980, 2011a) will be in doubt in this context, given that many of the citizens cannot read, and even those who do might not have the necessary exposure to invoke these principles. Thus, such principles assume an informed and exposed users who are capable of reading and performing basic tasks on computers and the Internet.

Similarly, trusted and user-centric identity management literature take for granted, a credible source document (e.g. Birth Certificate) integrity that could be used to support the acquisition of primary credentials. Regrettably, civil registration systems in developing countries and

Ghana in particular remain a challenge, with civil registration coverage at 71% (UNESCO, 2010).

On average, 63% of the adult population is literate in the region (71% of male adults and 54% of female adults). This varies from 29% in Niger to 94% in Equatorial Guinea.

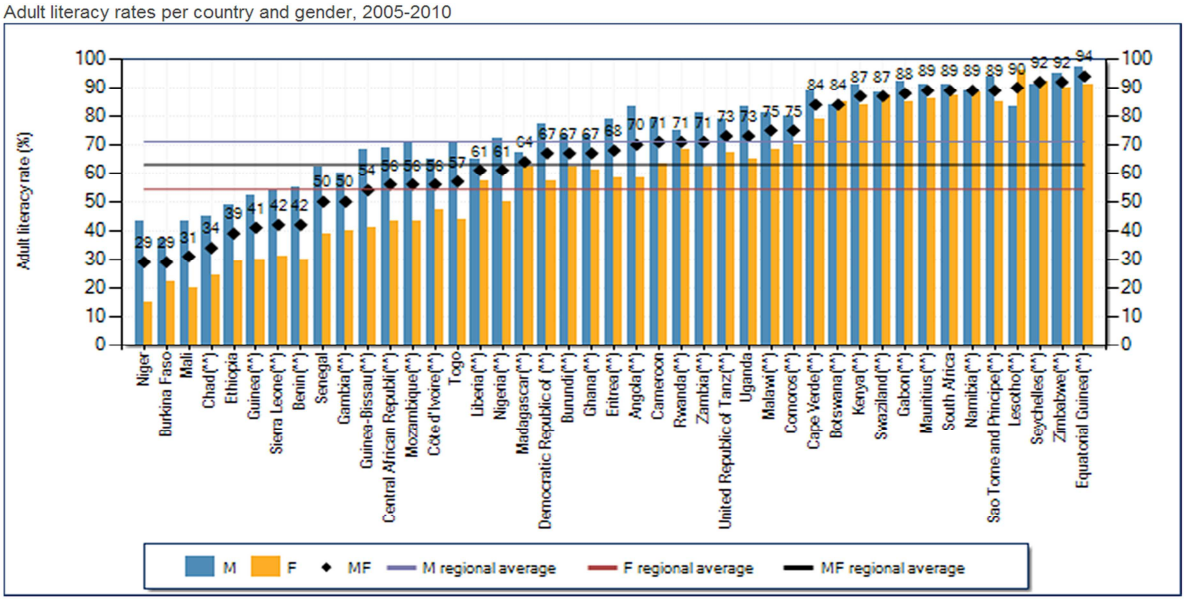


Figure 2 Adult Literacy rate in Sub Sahara Africa (Source: (UNESCO, 2010)).

Another phenomenon driving the theoretical analysis of IS success measures is the generation of customized experiences and personalisation of services as a result of the increased relevance of the internet in commercial transactions and social interactions. Primarily, Google, Facebook, and Yahoo! customize search results based on user location, browser used, and other user account settings in a way that two different individuals, using the same keywords in Google, would get different outcomes for their search results (Pariser, 2011). The IS success model is adapted in this study to address the above issues that remain to be addressed since it has never been applied specifically in IdMS context.

Empirical data for this study were collected from a series of interviews, stakeholder workshops and focus group discussions in Ghana, in addition to a quasi statistical analysis and media content analysis. This study highlights the important role of trust and information privacy in IdMS success. The study contributes to the identity management literature by enriching our current understanding of the key factors that affect successful implementation national IdMS and also provides guidelines for policy makers and developers. All the existing initiatives on effective means of identity verification and authentication depends on the context. For instance Internet connectivity and the speed of internet connectivity is taken for granted in many of such initiatives.

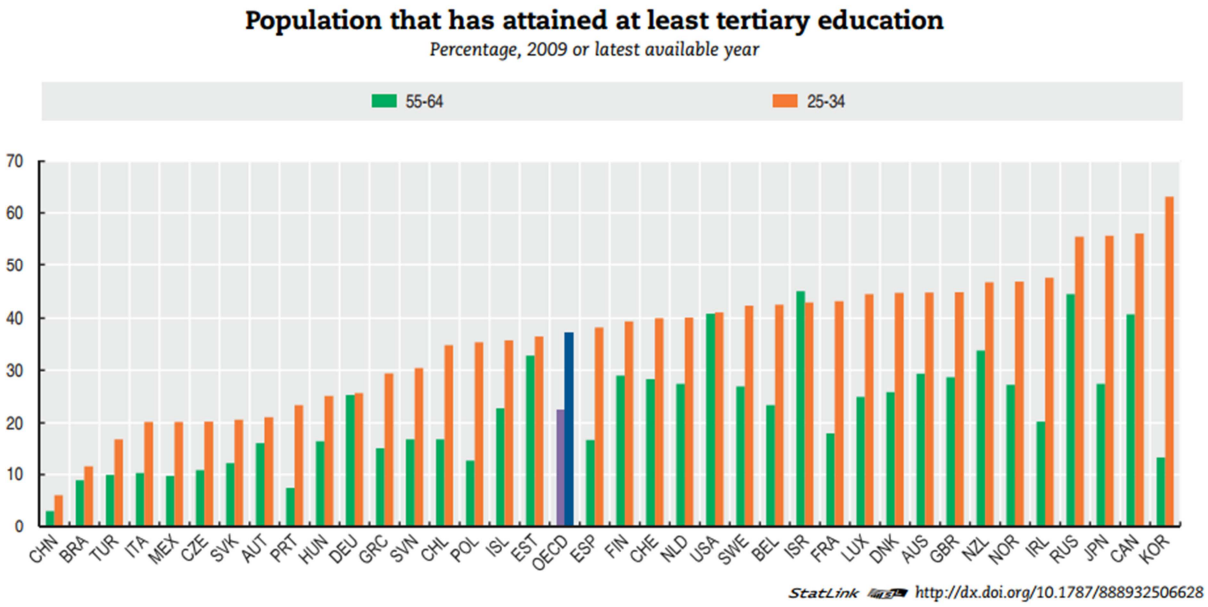


Figure 3 Adult Literacy rate in OECD countries (Source: (OECD, 2011b)).

1.2.1 Opportunities for Theoretical Contributions

Sarker and Wells, (2003) have posited that merely instantiating an existing theory in a new context can undermine the peculiar contextual issues (Sarker & Wells, 2003). This study refrains from such a practice by taking cognisance of the contextual issues in the application of theory.

The issues raised in the previous section highlight the theoretical gaps and also provide the following opportunities for theoretical contributions to IS success and Identity management literature and practice. In the foremost, effectiveness of IdMS in a societal context transcend technical architecture and perceived information quality. Thus the criteria used by organisations to measure success are not sufficient in the measurement of IdMS quality, given that the latter must address effectiveness from a multi-stakeholder perspective. In essence, IdMS effectiveness or success will also depend on the level of user involvement and how relying parties are able to collaborate in the use of the system for authorized secondary purposes. This study addresses such theoretical gaps in the measurement of IdMS effectiveness and legitimate secondary uses of personal information.

Secondly, "use" of IdMS may not be a good indicator of IS success, given that governments in many countries possess coercive powers in the enforcement of its policies (Turner, 2009, p. 47). The exercise of such coercive powers can make the "use" of IdMS mandatory. In such a situation, user satisfaction is what explains IdMS effectiveness. Trust in government and in technology is essential in ensuring user satisfaction, and thus a necessary precondition for the

diffusion of such technology, especially, in secondary and commercial uses of identity credentials and attributes. This study explains the role of trust in moderating the behaviour of citizens with respect to effective uses of IdMS. Thus, the inclusion of trust dimension presents a major opportunity for theoretical contribution.

Thirdly, in the physical world (face to face transactions and interactions) identity management (IdM) is critical in dealing with the associated risks, by helping to increase the confidence between parties to such transactions. IdM has thus been touted as a critical enabler of government to citizen interaction and the provision of access to social services (OECD, 2011c). In online interaction and transactions however, lack of a demonstrable link between a physical person and a "digital identity"[11] can create additional uncertainties that do not exist offline[12]. There has been a clarion call for the development of effective and efficient digital identity management strategies in order to harness the economic and social potential of the Internet and unleashing innovation to create trust-based digital services (OECD, 2011c). It is interesting to learn how and in what ways the contributions to economic development are derived in an economy and what factors can hinder such benefits in developing countries. This study can contribute new theoretical understanding about what factors must be considered in the introduction of IDMS in a developing country.

Moreover, effective uses of IDMS thrive on a high level of privacy protection that technology enables, and an appropriate level of assurance. Such privacy protection and assurance are also critical to further developing the market for online and in particular high value services. Ironically, many of the privacy principles fail to anticipate the possibility of educationally and technologically un-empowered users (de Villiers, 2005), a phenomenon common in many developing countries. For instance, user control and user consent as in the laws of identity (K. Cameron & Jones, 2007); and collection limitations and use limitation principles, specified in the OECD guidelines (OECD, 1980, 2002, 2011a). Highlighting these weaknesses in the existing privacy principles will strengthen the generalisability in their application and thus present a good opportunity to contribute to theory.

In summation, identification of the key factors that contribute to trusted IdMS from a developing country perspective, requires a critical analysis of the phenomenon within the context of its application and interacting with key stakeholders.

---

[11] Digital identity is an electronic or digital representation of a physical entity (person or object)

[12] Face to face transactions or transactions that does not involve the internet as a medium

1.3 Phenomena of Interest, Research Questions and Objectives

Researchers using deductive approaches often argue that a researcher must specify research questions prior to embarking on the inquiry. Others hold contrary views by arguing that prior specification of research questions are not suitable in exploratory and inductive research and thus hold in preference, the definition of the phenomenon of interest since the exploratory process can lead to the discovery of pertinent questions (M. W. Lewis & Grimes, 1999; Lincoln, Lynham, & Guba, 2011; Modell, 2010).

Ideally, this study should follow the second approach by merely focusing on the specification of the phenomena since this study takes the interpretive exploratory route. However, I do acknowledge the extreme importance of research questions for establishing focus in exploratory studies. Thus I first specify the phenomenon of interest in this section and then present the three interrelated research questions in the next section. All the questions largely fall within the bounds of the phenomenon as presented in the collection of papers that make up the thesis.

Taking a cue from the research background and the theoretical rationale, an outline of the phenomenon of interest which acts as a guide in all the phases of the study , which is also in line with the title of the study is as follows; "*trusted and citizen-centric national identity management system*". Thus, attention is given to understanding what constitutes IdMS success, the role of privacy concern and trust in fostering IdMS effectiveness within the identity ecosystem[13]. In the quest to understand the phenomenon, the researcher attempts to situate him/herself in the place occupied by the subject within the context in order to appreciate the situation on the ground (Bourdieu, 1996).

A combination of quasi statistics, open ended interviews, problem structuring methods using stakeholder workshop (Papamichail, Alves, French, Yang, & Snowdon, 2007; Sinkko et al., 2008) and focus group discussions (Kitzinger, 1995a; Krueger & Casey, 2009) will be employed in the acquisition of general comprehension of the context and social conditions. This approach gives the researcher a degree of control over the reality and the social mechanisms which exert their effects on the circumstances (Bourdieu, 1996). Secondly, the phenomenon

[13] Identity ecosystem is a trusted identity environment where individuals and organizations bounded by standards and policies for identifying and authenticating their digital identities, can transact and interact with confidence that the other party is not impersonating another person or taking undue advantange of the persoanl information exchange.

of interest focuses on shaping the behaviour of the key actors within the identity ecosystem by acknowledging the existence of different roles each actor can play to inculcate trust and confidence.

1.3.1 Research Questions

> The number of rational hypotheses that can explain any given phenomenon is infinite[14]
>
> Robert M. Pirsig

In spite of the extensive research on IdM, factors affecting citizen-centric IDMS implementation have not been adequately addressed (G. Aichholzer & Strauß, 2009; Dass & Pal, 2009). For instance, governments in many countries have invested in identity policies but identity abuses and lack of trust in government and technology remains a challenge, especially in developing countries. Ironically several innovative technologies professing to address many of such concerns have been implemented – touch2ID (Evry, 2010; Touch2ID, 2012), PrivacyABC (Sabouri, Krontiris, & Rannenberg, 2012), etc. It is therefore interesting to understand the major factors that affect the effectiveness of IDMS, and effective guidelines for addressing such fine-grained concerns will be very useful.

Formulating a research question is an intellectually challenging and time consuming undertaking (Saunders & Lewis, 1997). Yet the research questions act as a useful guide in shaping the research and as a tool for evaluation. I am therefore conscious of comprehensiveness and parsimony (Reay & Whetten, 2011; Whetten, 1989).

Question 1: The first research question focuses on understanding identity formation and the factors that contribute to its effectiveness or success. The ensuing question then is:

> *What are the major factors that influence (or contribute to) an effective or successful national identity management system?* Given the developing countries' perspective, it is also important to examine the *factors that influence identity management system's effectiveness in developing countries.* Various sections of papers one, two and three addressed this research question.

Question 2: The second question is in line with the second research objective and is as follows:

---

[14] By Robert M. Pirsig in his book 'Zen and the Art of Motorcycle Maintenance'

How does trust and information privacy concern affect the effectiveness of national identity management systems?

There is therefore the need to investigate the effects of citizens' concerns on the effectiveness of identity management systems. Addressing this question also involves an analysis of the nature of the relationship between trust and information privacy concern. Question two is addressed in papers two, four and five.

Question 3: The third research question is also in line with the third research objective and is as follows:

What measures must be put in place to ensure a trusted and citizen-centric identity ecosystem?

This question is based on the notion that given the multi-stakeholder perspective of national identity policies, it is important to define the common rules of engagement and the necessary assurances that can help in addressing the major stakeholder concerns.

1.3.2 Statement of Objectives

> The trouble with not having a goal is that you can spend your life running up and down the field and never scoring. — Bill Copeland[15]

The ambition of this inquiry is in threefold, to examine the trusted and user centric identity management systems that are privacy enhancing, understand the factors that contribute to IDMS effectiveness and to propose guidelines for instilling trusted identity ecosystem from a developing country's perspective. It is important to also know more about the formation of identity and their implication on the effectiveness of IDMS.

According to (Rojon & Saunders, 2012), in order to operationalise research questions, research objectives must demonstrate a "fit-for-purpose", and must be; comprehensible, specific, relevant, coherent, answerable and measurable. The objectives must thus be clearly linked to the study as a whole. Thus, the broad aim is divided into the following three specific objectives:

1. *Identify the key factors that contribute to the effectiveness of identity management systems.* A detailed analysis of the various factors that determine the success or effective-

[15] Bill Copeland was an Australian Test Cricket match Umpire

ness of IDMS is critical for a better understanding of design and identity policy considerations. The first research question is specified to address this research objective.

2. *Understand how and in what ways trust and privacy concern affect or contribute to the effectiveness of the IDMS.* Governments implement national identity management systems and identity policies in order to facilitate interaction, business transaction and to address information security challenges. Trust and information privacy concern have become a major subject in contemporary digital identity management discussions. Thus, a clear understanding of the role of trust and information privacy concern will ensure IDMS effectiveness. This will be an interesting addition to future identity policies and design guidelines.
3. *Propose guidelines for ensuring trusted and citizen-centric identity management system that is privacy enhancing.* The trusted identity management system depends on carefully crafted guidelines that address trust, regulatory and interoperability frameworks (Grant, 2011a), which takes into consideration, the context and the major concerns of all the key stakeholders within the identities ecosystem. Such an environment encourages legitimate secondary and commercial uses of personal information and the reliability of credentials and identity attributes.

1.4. Research Methodology

A summary of the research design which is an adaptation of (Crotty, 1998) is depicted in Figure 4. This study takes an interpretivist stance with a blend of pragmatic trajectory in understanding the factors that contribute to trusted and citizen centric identity management. Such a scientific paradigm enables the researcher to move beyond his horizon of understanding to see what is out there. This worldview is also significant since it reinforces the key attributes of the case study research strategy being adopted in this study. Thus, it opens an avenue for the researcher to gather evidence from multiple sources (Yin, 2008a, 2011a).

This study has been categorised into three integrated phases of inquiry – Phase 1, Phase 2 and Phase 3. Each of the phases entails a certain degree of fieldwork and desk research. The preliminary study, phase 1 involved gathering of empirical data using a combination of interviews and quasi statistics on citizens' perceptions and how identity credentials are used in developing countries. The interviews and the perception survey took place in Ghana. A combination of interviews and stakeholder workshop (forum) was used to gather empirical data during phase 2. The aim of this phase of the research was to investigate how personal information could be used for legitimate secondary purposes. This study was also an opportunity

to identify the major stakeholders and the effect of trust and privacy concerns on effective uses of IdMS. Phase 3, data validations exercise, entailed the use of interviews, focus groups and a follow-up stakeholder workshop. The objective was to develop a guideline for crafting a trusted identity ecosystem. Thus I needed participants' account of their experiences in using the various credentials and how it has affected their lives and interactions and business transactions. I employed Interpretive Phenomenological Analysis (IPA) (Creswell, 2007a; J. A. Smith, 2004; Thorpe & Holt, 2007) as a means of forming and attaching meanings to what participants said. A detailed account of this interpretation approach is in chapter 4. Figure 4 provides a snapshot of the philosophical paradigm and the methods adopted in this study.

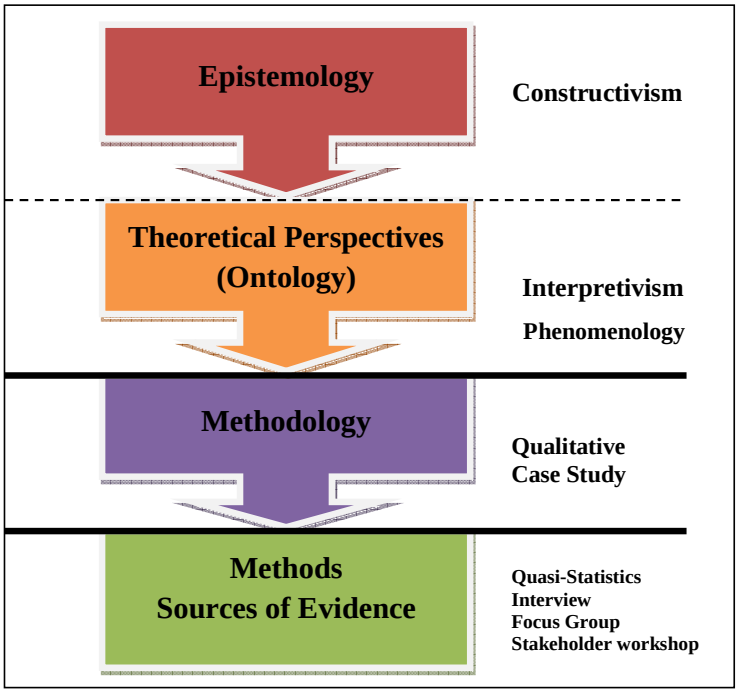


Figure 4 Research Paradigm & Methods. Adapted from (Crotty, 1998).

1.5. Summary of Findings

The findings of this thesis are already published in three peer-reviewed academic conference and three peer reviewed academic journal papers. Table 1 summaries the various research questions, objectives, and the findings of each of the six papers published during the course of the study. The table also indicates names of co-authors where there was a joint publication and the nature of the co-author contributions.

Paper	Author	Title	Research Objectives	Research Question Addressed	Summary of Findings
1	Adjei & Tobbin	Identification Systems in Africa; The Case of Ghana	Explore the factors IDMS uses in developing countries	What underlying factors motivate or inhibit IDMS implementations	Connectivity, taxation and political motives are key factors that can affect effective uses of IDMS

Paper	Author	Title	Research Objectives	Research Question Addressed	Summary of Findings
2	Adjei & Olesen	Analysis of Privacy-Enhancing Identity Management Systems	To understand the relationship between individuals' intentions to disclose personal information, their actual personal information disclosure behaviours.	What are the major issues involved in the design of privacy-enhancing IDMS. What design principles must be observed?	- Perceptions of privacy and trust are major factors that affect acceptance of IDMS. -Country specific nature of privacy laws limits their ability to address digital identity issues giving the ubiquity of the internet.
3	Adjei & Olesen	Keeping Identity Private; Establishing Trust in the Physical and Digital World for Identity Management Systems	To understand the major issues involved in the design of privacy-enhancing IDMS and contribute to improved framework and design principles.	What design principles must be observed in the design of privacy-enhancing IDMS?	Many of the privacy initiatives does not address privacy issues in face to face transactions which is a major focus IDMSs in developing countries.
4	Adjei & Olesen	Secondary Uses of Personal Identity Information: Policies, Technologies and Regulatory Framework	To provide a means of communicating identity-related concepts to policy-makers, users and technologists.	What constitute personal information and what are the major user concerns in relation to secondary uses of personal information?	Efficient civic registration system, user collaboration and regulatory framework encourage effective secondary uses.
5	Adjei & Olesen	Building Trusted National Identity Management Systems – Presenting Privacy-Concern Trust Curve	To understand the key stakeholder concerns regarding the collection, storage and use of personal information and how such concerns should be addressed to ensure trusted identities.	How should stakeholder concerns be addressed in a trusted identity management system?	To ensure trusted identity ecosystem governments must strenghten civil registrations which is the key source document for identity formation. Policy makers must also strive to attain the trust threshold.
6	Joseph K. Adjei	Towards a Trusted National Identities Framework	To identify the key requirements for crafting a trusted identities ecosystem	What are the key requirements for crafting a trusted identities ecosystem?	Institutional cooperation and user empowerment are critical in a trusted identities environment

Table 1 Summary of Findings

1.6. Outline of the Thesis

The thesis has been logically categorised into four sections as follows; 1) Introduction and Research Context; and it is followed by 2) Theoretical Framework and Research Methodology; 3) Findings, Discussion and Conclusions further work; and 4) Appendixes, showing the

paper publications during the study. An outline of the various chapters of the thesis are as follows:

– Chapter 1 – Introduction. This chapter provides a background to the study and the theoretical rationale. An outline of the phenomenon of interest is provided in addition to the research question, the objectives, a summary of the research methodology and findings. The chapter concludes with a summary of the structure of the thesis.

– Chapter 2 – The research context and the state-of-the-art: This chapter provides an overview of the concepts necessary to the understanding of user-centric identity management systems, the contextual issues in Ghana and the Danish civil registration system. An overview of existing IdMS technologies, and the concepts of trust and information privacy are presented in this chapter.

– Chapter 3 – Theoretical Framework: this chapter begins with a discussion of IS success and then introduces the various theories in relation to success and effectiveness. An overview of the DeLone and McLean IS success model is presented in addition to the implications of its application in the measurement of IDMS success.

– Chapter 4 – Research Approach and Methodology: This chapter explains the philosophical paradigms, research philosophy and the methodological considerations of the study. The research design, sources of evidence and data interpretation principles are also presented in this chapter.

– Chapter 5 – Findings and Contributions: This chapter is an integrative summary of the findings, contributions and the lessons learnt from each of the papers written in the course of the study. The chapter also explains the research contributions organised according to the selected publications.

– Chapter 6 – Discussion and Research Limitations: A reflection on the work presented in the thesis is presented. We discuss the most important contributions and the main problems encountered in the course of the thesis. Furthermore, we present some challenges and problems in the area of user-centric service composition and delivery. Following the discussions is a list of papers published in the course of the PhD study.

– Chapter 7 – Conclusions and Research Limitations: This chapter presents the conclusions drawn from the study and the research limitations. Copies of the publications are in the appendix.

Chapter 2: State-of-the-Art and Research Context

Webster and Watson (2002) have posited that an effective literature review creates a solid foundation for advancing knowledge and also uncovering those areas in need of more research (Webster & Watson, 2002). This Chapter and Chapter 3 provide such a review and, thus, offer a theoretical basis for the research. The chapter begins with an analysis of the concepts of identity, digital identity, and identity management, and their implication on personal information exchanges in citizens interactions and transactions. It continues with a review of literature on trust and privacy and the developments in OECD in that regard. An overview of the civil registration system in Denmark and the existing identity management situation in Ghana then follows.

2.1 Identity, Identification and Identity Management

2.1.1 Identity

Identity and identification have been used interchangeably by researchers and in conversations, but recognising the distinctions is of relevance to the study of identity management. The concept of identity has over the years been discussed from the perspective of technical scientists, psychologists, sociologists, etc. From a mathematical perspective, Leibnitz defined identity on the basis of whether two things can be distinguished from each other (Feldman, 1970; Wilton, 2008a). Thus, two objects sharing similar characteristics like shape, extent, position in time and space, could be deemed to have or share the relationship of identity (Feldman, 1970). Similarly, in his narrative of identity, Ricoeur (1991), described the the notion of "identity" as involving two opposing realities (Ricoeur, 1991) – the identity "selfhood" (in Latin ipse), which refers to those attributes that makes a person unique; and the identity sameness (in Latin idem) referring to the attributes that will persist and thus keep a person the same. Crompton (2004), simplified such descriptions by positing that, identity is the relationship between something and itself (Crompton, 2004).

In relationships, people usually resort to either self identity or sameness as a means of recognizing people or differentiating them from others. This notion of identity is vital in the formation of better knowledge of people which is essential in building trust, a necessary foundation in governance, commerce and social interactions. A person's identity is regarded as a reflection of those things, which are generally known about them by the people with whom they interact (Wilton, 2008a). Identity in information systems therefore consists of traits, attributes, and preferences, based on which an individual may receive personalized services either online, on mobile devices, at work, or in many other places (Liberty, 2004). In essence,

identity is the chain of events from enrolment and credential issue through to credential presentation and thus, information about an entity that is sufficient to identify that entity in a particular context (Bertino, 2012).

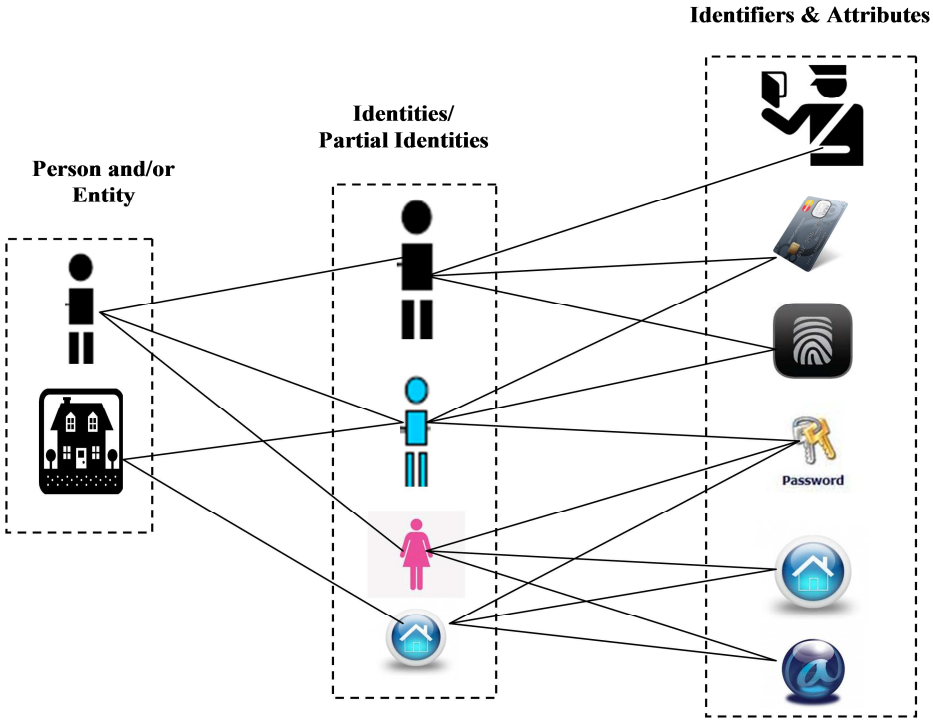


Figure 5 Entity, Identity, Identifiers and Attributes

2.1.2 Digital Identity

In our day-to-day physical interactions and on the Internet, we leave our footprints in the form of pieces of information about ourselves, which accrete in various ways over a period of time. These footprints (also referred to as Partial identity as illustrated in Figure 6) are the trails from e-mails, visiting websites, purchasing items on the internet, postings and comments on Facebook and other social networks, text messages, our information in various databases. Such a phenomenon implies that, a person or an entity can have many different personas[16] depending on the context, which fundamentally redefine the notion of identity.

Digital identity is therefore a set of claims made by one digital subject about itself or another digital subject. In the the words of Turkle, digital identity refers to "the sameness between an entity and its persona" (Turkle, 1997). It is also the essential and unique characteristics of an entity that is used to identify it (Abelson & Lessig, 1998). Thus, Digital identity is the digital

[16] Persona is a model of an individual's public personality based on data and maintained by transactions, and intended for use as a proxy for the individual (Roger Clarke, 1994)

representation of the information known about a specific individual, group or organization. Such information encompasses not only the attributive information (i.e. social security number, date of birth, and country of origin), but also biometrics data (i.e. iris or fingerprint features), and information about user activities, including Web searches and e-shopping transactions. Such definitions have widened the concept of identity to include identifiers (Figure 5) such as login names and pseudonyms. Hence, the specific sets of identity attributes and identifiers used to carry on a specific transaction in cyberspace can vary considerably and therefore digital or electronic identity is now seen as an electronic representation of a real world entity or, an online equivalent of an individual (Roussos, Peterson, & Patel, 2003).

Digital identity thus removes the requirement for parties to be present during transactions and interactions. This is what Rahaman & Sasse, (2011) refer to as *disembodiment of identification processes* (Rahaman & Sasse, 2010). Digital identity in effect, ensures a lack of confinement to a particular location or network and thus ensuring wider, distribution of personal information (Camp, 2003). It is therefore important that such factors are also addressed in identity policy to cater for the resultant differences between digital and physical identity (Taylor & Lips, 2008).

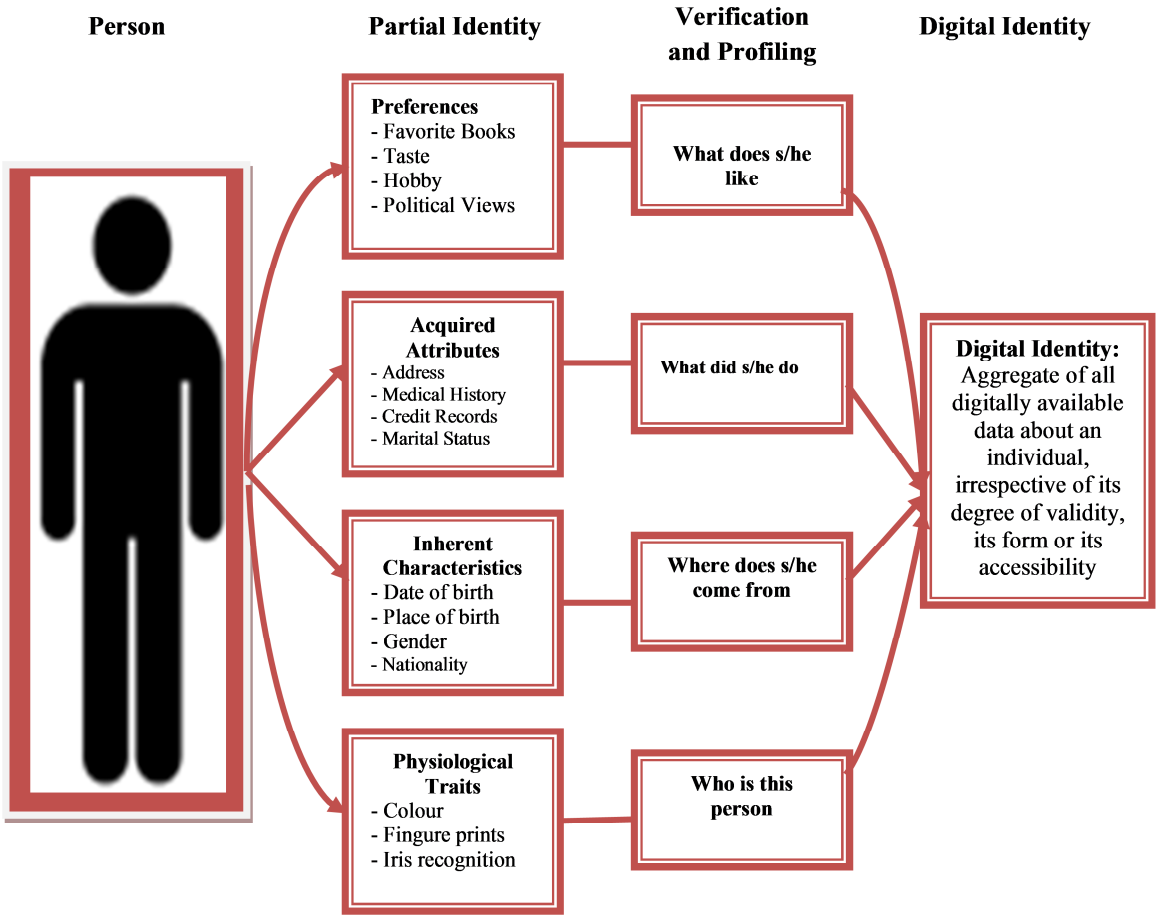


Figure 6Digital Identity.

2.1.3 Identification

Due to the complexity of modern business transactions and social interactions, each party would like to ascertain, with a certain degree of confidence, the assurance of the credibility of the people with whom they are dealing. Such a desire for a more sophisticated knowledge of transacting parties has increasingly become necessary given that the Internet was built without a way to know who and what one is connecting to (Kim Cameron, 2005). Interestingly, this concern was as captured in a 1993 cartoon as in Figure 7, which appeared in a New Yorker magazine as; "*on the internet nobody knows that you are a dog*" (Steiner, 1993).

Identification is therefore a process of establishing the identity of; or recognizing or treating a thing as identical with another; or establishing as being a particular person or entity (*Concise Oxford Dictionary*). It is also the act of making, representing to be, or regarding or treating a thing or entity as the same or identical. Thus human identification is the association of data with a particular human being (R. Clarke, 1994), the process of linking information with a particular person, or action of being identified (Crompton, 2004). In effect, identifying an individual requires a clear focus on the distinctive characteristics or attributes of the individual (i.e. Names, date of birth, address and identifiers like driver's license number). The person must be able to demonstrate knowledge of something (something you know – e.g. a password); possession of a token or credential (something you have – e.g. driver's license); or by means of physiological characteristics or features (something you are – e.g. gender, facial features, signature, fingerprint) (Crompton, 2004).

If identification is a process, then the integrity of the identification process and its usefulness will depend on: the reliability of the registration or enrolment processes, how difficult it is to duplicate or alter credentials; and the ease of verification of the link between the issued credentials themselves and the person presenting it. An efficient identification must observe the following:

- The issuer of assertion must be unequivocally identifiable from the token.
- The data subject of an assertion should be also unmistakably identifiable. Thus, it should be difficult for someone to reuse stolen tokens.
- Tokens must be tamper resistant, or difficult to forge or vary after it is made or issued.

To meet such identification criteria, an efficient system for managing identities will be necessary.

On the internet, nobody knows you're a dog

Figure 7 On the internet nobody knows you are a dog.

Developing the identity metasystem concepts as an integrated framework to support different identification technologies and identity platforms in a standardised manner Cameron, (2005) proposed what he called the laws of identity which is seen as a very good foundation for constructing the identity layer. An outline of the laws of identity are summarised in Table 2.

PRINCIPLE	BRIEF DESCRIPTION
User Control and Consent	Technical identity systems must only reveal information identifying a user with the user's consent
Minimal Disclosure for a Constrained Use	The solution that discloses the least amount of identifying information and best limits its use is the most stable long-term solution Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.
Justifiable Parties	Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.
Directed Identity	A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles
Pluralism of Operators and	A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers[17].

[17] Identity provider is an organisation responsible for the process of enroling and issuance of credentials to individuals which can be used as proof of identity.

PRINCIPLE	BRIEF DESCRIPTION
Technologies	
Human Integration	The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks
Consistent Experience Across Contexts	The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

Table 2 The Laws of Identity (Kim Cameron, 2005) .

The aim of these identity management design principles is to give users control and allow them to make decisions that reflect their preferences such as being able to understand and agree to the uses that the organisation makes of their personal information. It does not however, consider the reasons why an individual might be reluctant to provide certain information to certain parties.

2.1.4 Identity Management Systems

Regardless of who makes the identity claim, it is important that the claims are packaged in a transportable token such that the data subject or the identity service provider will not always need to be available in real time. An efficient system is therefore needed to manage such requirements. Throughout history, different variations of Identity management systems were used to establish the basis for trade and governance by means of tokens and technologies, seals, coded messages, signatures, jewellery, etc. (3G_Americas, 2009).

Due to increased modernization and trend in technological development towards online transactions and interactions and via single sign-on (SSO) (G. Aichholzer & Strauß, 2009), the need for efficient and effective user identity management systems have become imperative. Digital identity management aims at transcribing to the digital world, models of interaction which have been used for centuries in direct face-to-face communication schemes in order to enable trusted remote interactions.

Van Thuan (2007), described electronic identity management as *"the processes, policies and technologies used to manage the complete Lifecycle of user identities across a system and to control user access to the system resources by associating their rights and restrictions"*. In effect, Identity management systems, consist of the processes and all underlying technologies for the creation, management and usage of identities and their attributes. Invariably, the objective of electronic IdM is to ensure consistent business rules and practices; tightening of control over user-to-applications; automation of business processes in order to minimize op-

erational costs; enhanced security; improved productivity. (Lips & Pang, 2011) have therefore suggested a shift in focus towards analyses of the wider societal implications of IdMS and related social design issues.

Figure 8 illustrates identity formation process and a summary of which is as follows:

i) Enrolment or Registration - Individuals must go through an initial registration or enrolment processes where their biographical footprint, biometric footprint or a combination of both are captured into the system. The outcome of the enrolment process is the issue of credentials or identifiers to those registered. In effect, enrolment is the process by which an individual is brought within the identity policy and the resulting systems and the eventual issue of credentials and identifiers. The birth of a child or the arrival of a qualified foreign national will usually trigger the enrolment process in a national IDMS.

ii) Authorisation – upon registration, permission and privileges to access the resources and services are assigned to an individual based on a predefined identification policy.

iii) Authentication – This is the process of establishing with a certain degree of confidence in the user's identity or a process that results in a person being accepted as authorized to engage in or perform some activity (E. A. Whitley, 2009). Thus, authentication is the process of verifying that a user is who he/she claims to be. To gain access to services and resources, the individual makes a verifiable identity claim by either logging into a system with a given credential, knowledge of certain information, or based on biometric data. There are many authentication methods with different levels of assurances, also referred to as authentication factors, such as: something the user knows (i.e. Password); something the user has (i.e. Smart card or passport) and or something the user is (i.e. Biometrics) (van Thuan, 2007).

iv) Access Control – Authentication process results in the access control *process* in which a check is made by the system to see if an individual has a valid authorisation to access the resource;

v) Revocation – on the expiry of individuals' rights or when a person is no more associated with the system, a revocation process is triggered resulting in the credentials and associated rights being rescinded. Such circumstances include the death of a citizen, completion of school or travelling outside a country for more than a specified period.

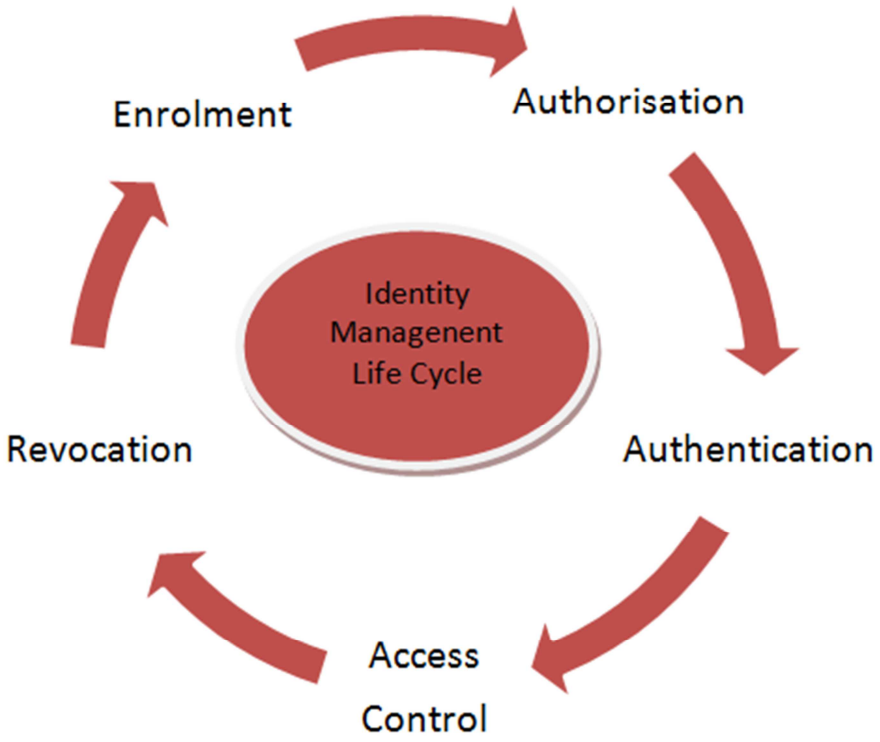


Figure 8 Identity Management Life Cycle.

2.1.5 Identity Verification

Verification is the means by which an identity credential presented by an individual is checked by either identity issuers or relying parties. At its simplest, this might simply involve looking at a card and accepting it if it appears genuine. Alternatively, various checks on the validity of the credential may be undertaken. These can include a consideration of specialised security markings on the credential or contacting an identity assurance agency to check that the credential is still valid and not listed as stolen or expired. In some cases, the verification process may be against information held on the credential; in other cases, the check may be against data held by the identity service provider. The verification process require efficient and effective user identification and authentication, making IdM a crucial challenge in e-government.

2.1.6 Biometric Authentication

Biometrics are measurable physiological and behavioural characteristics which can be used for identity authentication and verification. Various forms of biometrics can be digitised and used to automate human recognition. However, due to privacy, technical, legal and many other challenges, certain biometrics are not commonly used. For instance, Jain et al., (1999) identified universality, uniqueness, measurability, performance, acceptability and circumvention as the key factors in assessing the suitability of any trait of characteristics to be used for

biometric authentication (A. Jain & Aggarwal, 2012; A. K. Jain, Bolle, & Pankanti, 1999; Wayman, Jain, Maltoni, & Maio, 2005).

Biometrics which are commonly used in practice for IdM purposes include fingerprint, voice recognition, facial recognition, finger and palm veins (Gutwirth, 2012). Biometrics authentication usually does not depend on the possession of a physical credentials or tokens, and memorisation of certain identifiers (i.e. user names and password), and thus offer attractive options for strong authentications.

However, it can be vulnerable if the threshold is not set properly. Such vulnerability can be avoided when biometrics are used in conjunction with other credentials, including additional types of biometric or multiple biometrics. Thus the strength of biometrics is increased when it is augmented with multiple factors (van Thuan, 2007).

Given the sensitivity of biometric data, its frequent use online requires a consideration of the rights of individuals, the identity providers and relying parties and the responsibilities of law enforcement agencies. On the part of data subjects, maximum control could permeate from limiting uses of biometrics to situations where the data subjects is in control, such as storage of encrypted format of the biometric on devices in the possession of data subjects.

Biometric systems can be applied in either a verification mode or an identification mode depending on the context. The application of biometric systems in a verification mode implies that, the system will validate the identity of a person by comparing the captured biometric data with an already stored biometric template of the person (A. K. Jain, Flynn, & Ross, 2010; Li & Jain, 2011).

Its application in identification mode on the other hand is where the system attempts to recognise an individual by conducting a one-to-many search and comparisons through the templates of all the users who are registered in the database for a matching template. The objective of identification mode of biometric application is to establish a person's identity and thus preventing her from using multiple identities. A failure of the system to match implies that, the data subject has been registered. Such a condition is very critical in negative recognition situations, where there is the need to establish whether a person is who he/she (implicitly or explicitly) denies to be (A. K. Jain et al., 2010; Li & Jain, 2011).

Figure 9 is a biometric block diagram illustrating a biometric authentication system in both verification and identification modes. In the verification mode, the system performs a one-to-one comparison of captured biometric data with a specific template that is stored in a biometric database in order to verify an individual is who he/she claims to be. The following

three steps are observed; in the first place reference models, for all the users are generated and stored in the model database.

Secondly, sample data is matched with the information in the reference model to generate the valid and invalid acceptance and rejection thresholds. The final stage, which is the testing of validity using various forms of credentials and identifiers (i.e. smart card, user name, identification number, etc.), to indicate the template to be used for comparison.

In the identification mode, a person is first enrolled in the biometric system where biometric data is captured and stored. Subsequently, biometric information is detected when the person attempts to use the system and the data is compared with the information stored during enrolment.

In Figure 9 the sensor which is usually an image acquisition system is the interface between the real world and the system, the next block, performs all pre-processing activities like removal of background noise in order to obtain a normalized data. In the third block, necessary features are extracted. Feature extractor is the stage where correct features are extracted in an optimal manner in order to create a template. A template is a synthesis of the relevant characteristics extracted from the source. Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the file size and to protect the identity of the person. During enrolment, the template or a card is stored in a database and is used as the benchmark for matching by parsing the template to the matcher for comparison based on the predefined algorithim.

Biometrics are very useful in the identification and removal of duplicate names and attributes from an existing IdM database.

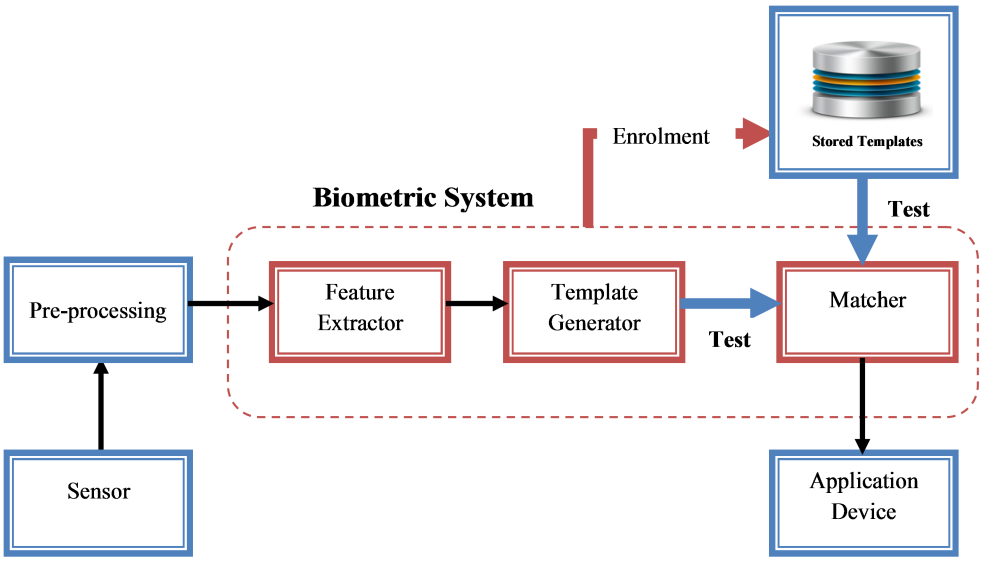


Figure 9 Biometric System.

2.2 Models of Identity Management Systems

Various forms of digital identity management systems have been implemented using various technical and architectural model. This section discusses some of the popular identity management models – silos, centralised, federated and user-centric identity management models.

2.2.1 Silo Identity Systems

The soiled identity management system is an IdMS model, that is usually designed and operated independently by an organisation, mainly to fulfil its primary objectives, such as active directory. Such an IdMS usually does not allow connections with other IdMSs and thus the identity provider also takes the role of service provider (SP), such that it manages the name space and authentication tokens for all its users. The SP also authenticates users based on their identifier-token pairs during service access. Users can be allowed to define their own identifiers, as long as they are unique within the name space. A major benefit of the silo model is unlinkability. Given that the system is not connected to any other system, user attributes in one system cannot be easily linked to different identifiers of the same users in other domains (Donohue & Carblanc, 2008).

Additionally, a security breach in one silo does not compromise security in other systems. Silo systems are however very rigid in that they do not afford users the convenience of linkability where necessary, resulting in the use of a multiplicity of credentials and identifiers depending on the context. Such multiple user accounts, identifiers and credentials are usually very difficult to manage and thus users resort to the use of similar identifiers across different silos with its propensity to vulnerability of the systems. Another disadvantage of the Silo

model is waste of resources, because of resource and effort duplication. For instance, a person's details are stored in each of the identity silos although this could be avoided if information were to be shared.

Although there may be genuine reasons for keeping identity information in silos, the organisation in any sense, wastes resources and duplicate efforts in trying to separate user profiles (Donohue & Carblanc, 2008).

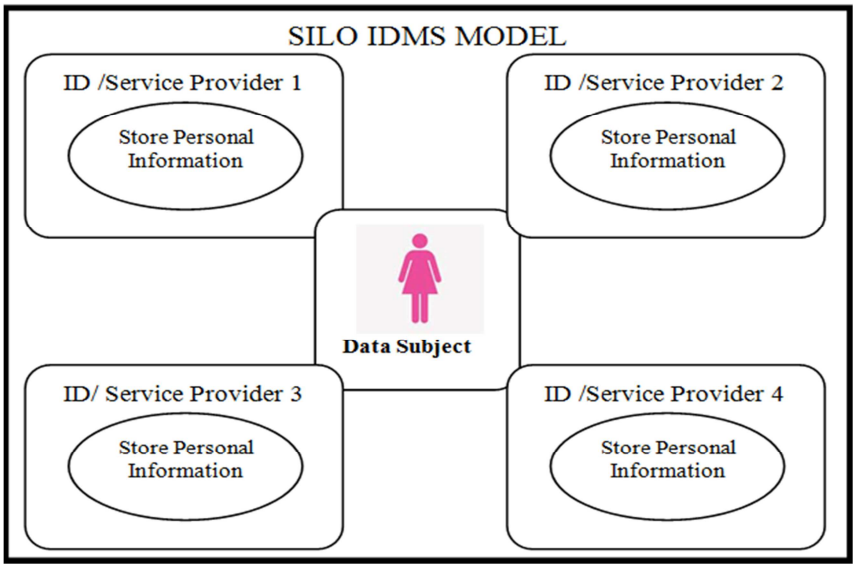


Figure 10 Silo Identity Management Model.

2.2.2 Centralised identity systems

The centralized IdMS model is an early attempt to rectify the inherent limitations of silo systems by centralising the independent databases into a single system. Thus in the centralised model, user data are kept independent of the various application silos, and data are made available to service providers from the central database. Due to the centralised nature of the systems, each user can use the same credentials and identifiers to access different services, whilst all the providers authenticate the client through the same certificate before granting access to their services. Centralised IdMS have evolved with time, given the increasing need to share and reuse identity information. Centralized IdMS is a very common model for storing and managing digital identities (Donohue & Carblanc, 2008).

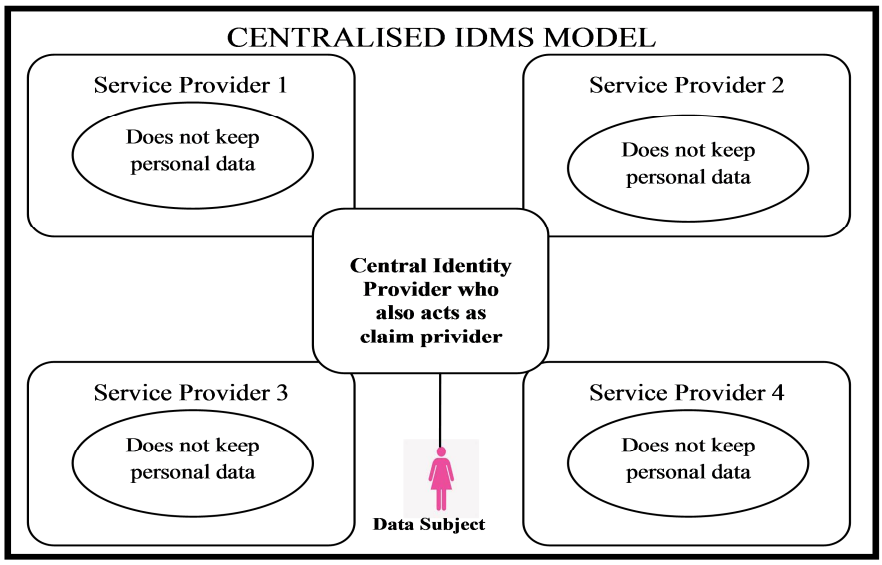


Figure 11 Centralised IDMS Model.

2.2.3 Federated Identity Systems

Federated identity management model seeks to simplify the account management problems pertaining to silo model. Instead, service providers do not aggregate their account information as in the case of centralised models. Rather, service providers establish a central "identity provider" which manages user identifiers by linking identifiers based on sets of predefined rules of engagement among federation of SPs who were previously unlinked.

Federated IdMS started as a response to trust and privacy issues of the centralised IdMS (Donohue & Carblanc, 2008). Users belonging to identity federation can access services by authenticating to the central identity provider, by allowing a user to obtain seamless access to services from all the service providers belonging to the federation. Thus in federated IdMS model, the identity provider could also be a service provider.

In a federated IdMS environment, users do not need to exhibit various identifiers and remember different user names and passwords, because a single authentication event at the primary account also gives them access to multiple service providers. Similarly, members of a federation do not need to create multiple accounts for users prior to offering services. The identity provider is able to facilitate seamless data sharing between two or more accounts of the same user because it knows which identifiers correspond to the same user, and thus making the identity provider a trusted third party.

Federation can be more convenient for users and efficient for the organisations managing the accounts, but it also gives rise to new challenges. For example, it may not be easy to enable information sharing between organisations that do not have a pre-established relationship, but from whom an individual would like coordinated service delivery. This problem has recently

been addressed using contractual and policy models to supplement the technology in order to help mediate relationships between unknown parties.

However, if the identity provider chooses not to establish a federation relationship with users' preferred service providers, users may be unable to use their federated accounts to access those service providers. Another challenge relates to the problem of determining liability for these complex business relationships and protection against theft and errors. The main vulnerabilities stem from the fact that the identity provider knows which identifiers correspond to a given user. Thus, such knowledge places the identity provider in a position where it could impersonate the user or enable others to do so.

Some of the popular browser-based federated identity initiatives focusing on single sign-on[18] (SSO) include: the OASIS Security Assertion Markup Language (SAML) 2.0 (OASIS, 2012), the Liberty Alliance project (OASIS, 2004), Microsoft_ Passport or windows Live ID (Microsoft, 2013; Westfall, 2011), the Shibboleth Initiative (Shibboleth, 2013), and OpenID (Eldon, 2009).

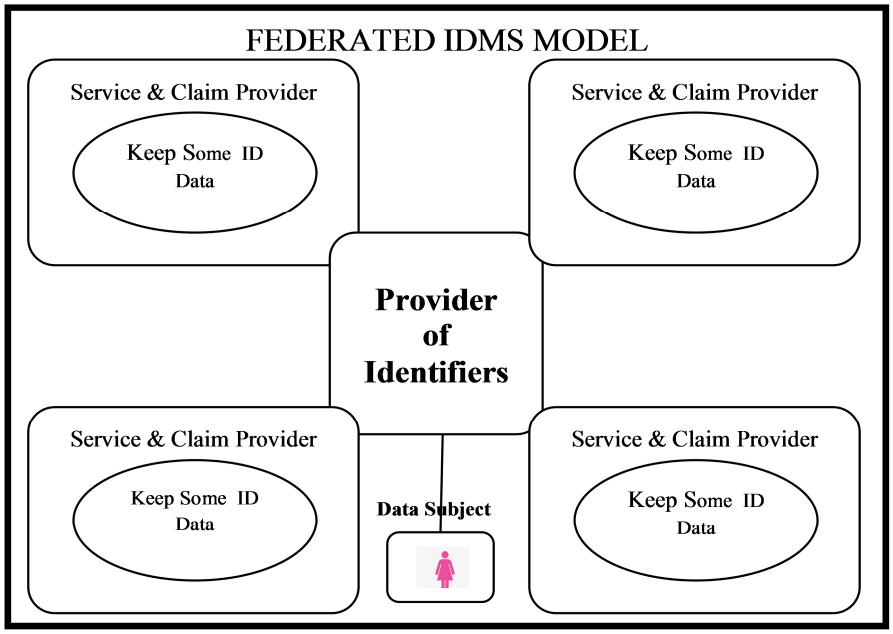


Figure 12 Federated IDMS Model.

[18] Single Sign-on is a federated identity solution that allow clients to perform a single log in operation to an identity provider, and are yet able to access resources offered by a variety of service providers (Armando et al., 2012).

2.2.4 User-centric identity systems

User-centric identity system is an attempt to give users maximum control over their personal information (Kim Cameron, 2005; Cavoukian, 2012). Thus, User-centric IDMS seek to offer users the flexibility to choose identity providers independent of service providers, and do not necessarily need to provide personal information to potential service providers in order to obtain access to services and resources. In such a model, the roles of Identity providers is that of a trusted third party who store user account and profile information and authenticate users, and service providers accept assertions or claims about users from the identity providers.

User-centric model are also designed to ensure that identity providers operate in the interest of the users rather than in the interest of the service providers. In a user centric model, service providers do not necessarily form part of an identity federation. Thus service providers merely become "relying parties" with users being able to choose what information to disclose when dealing with service providers in particular transaction.

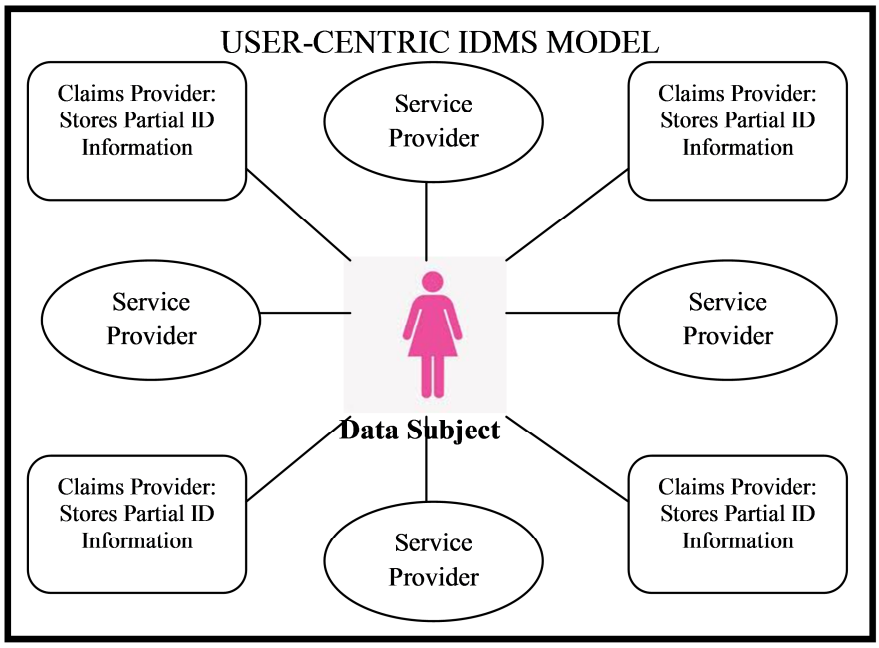


Figure 13 User-Centric Identity Management Model.

Similarly, although service providers require users' personal information to process a transaction, individuals use different identity providers, and different identity attributes, and thus information is not stored in one location. The role of identity providers becomes that of a trusted third-party, since users will usually trust a broker they can control; whilst relying parties will not trust a broker if the claims asserted are actually self-vouched by the user (Donohue & Carblanc, 2008; Jøsang & Pope, 2005).

Various innovative user-centric IdMS solutions have been tested with appropriate steps to address the concerns of both the user and the service providers as described in section 2.2.5.

Table 3 provides a summary of the key attributes of the IdMS models described in this section

Process	Silo	Centralised	Federated	User-Centric	Trusted Identity Ecosystem
Method of Authentication	Users must authenticate to identity providers who are also service providers in each transaction.	Authentication is to a centralised account.	Users authenticate to one identity provider and access services across the federation.	Users authenticate to identity providers, and service providers have to rely on that authentication	Various authentitcation schemes available depending on the assurance required
Location of Identity Information	Information is stored by each Identity Provider.	Identity information is stored in a central Identity directory.	Identity information held by each participant of the federation with whom a user enrolled. Access to services is based on federation's agreements.	Identity information is stored by identity providers chosen by the user. Service providers rely on identity providers.	Identity information is stored by users preferred identity providers including social networks
The method of linking accounts/ learning if they belong to the same person	Accounts are kept separate and are not linked.	All identity attributes and detail of identifiers stored in a central register. Thus linking is not necessary	Each identity provider determines which of user attributes and identifier should be linked to other federation members' accounts	Uses of cryptography can prevent linkages between a user's different digital identities, leaving the user in control.	User involvement in identity policy and uses of cryptography to give users maximum control control over personal identity information.
Trust / Privacy Implications. Nature of dependency	User relies on each service provider to protect personal information. Absence of information sharing is a privacy advantage.	The user is reliant on the service provider to maintain the privacy and security of all of his or her data.	Users have rights from contracts, but they may be unfamiliar with options. The federation has leverage as it is in possession of the user's information.	Users can keep accounts separate and still allow information to flow, but bear greater responsibility.	Various trust frameworks and institutional cooperation schemes available
Convenience	Silo accounts are inconvenient for users and service providers due to multiple authentications, redundant entry of information, and lack of data flow.	This arrangement is easy for the user since he or she only has to deal with one credential to call up the account and since he or she has to authenticate just once.	Other members of the federation avoid the burden of credential management. Businesses that provide services to a user can coordinate service delivery.	Users may be ill equipped to manage their own data (also a vulnerability) and may need training and awareness raising.	Interoperability at all levels
Vulnerabilities	Silo systems offer the advantage of having limited data on hand, thus creating less of an incentive to attack. They also have a better defined and stronger security boundary to keep attackers out and limit exposure from failures.	Risk of single point of failure as ID provision from a central location. The the central register is susceptible to attack given that entire user profile is stored in one location and other entities are unable to check for validity.	Users have little input into the business-partner agreements. Some service providers will set up federation systems to exploit users. Currently there is no way to safeguard data after it has been shared.	Concentration in the market for identity providers could leave them with much power. Currently there is no way to safeguard data after it has been shared.	Trust threshold ensures that certain level of privacy maintain at all times

Table 3 Summary of IDM Models: Adapted from (Donohue & Carblanc, 2008).

2.2.5 Privacy-Enhancing Technologies

In a user-centric IDMS, the issue of distrust between the user and the relying party is addressed, because the identity provider acts as a trusted third-party broker. Individuals can

have several different identity providers, and for that matter, their information may not be stored in one place.

U-Prove (Microsoft, 2011), IDEMIX (IBM, 2010), OpenID (Recordon & Reed, 2006) and OAuth (Hammer-Lahav, 2009) are some of the major user centric and privacy enhancing IdMS technologies and frameworks that seek to assist transacting and interacting parties to manage claims and attributes so that the relying parties are assured that the information is correct before engaging with the user, although the identity of the user might not be revealed. These approaches ensure minimum disclosure of personal information and fine-grained delegation of authorization between service providers. An overview of the technologies is provided in this section.

U-Prove – Developed based on an advanced cryptographic technology and concepts, U-Prove is an attempt to overcome the age old dilemma between identity assurance and privacy as discussed in (Donohue & Carblanc, 2008; Microsoft, 2011). The dilemma is addressed by enabling minimal disclosure of identity information in electronic transactions and communications. U-prove is a technology that Microsoft, the developers, believes could assist in their promotion of an open identity and access model for individuals, businesses, and governments agencies. Thus the concept of U-prove is rooted in the principles prescribed in the identity metasystem (K. Cameron & Jones, 2007; Kim Cameron, 2005). For instance to satisfy the minimum and selective disclosure principles, the U-Prove agent software acts as an intermediary between websites and thus, allowing users to share data in a manner that protects their privacy. U-Prove also provides the mechanism for separating the protocol for information retrieval from trusted third parties from the protocols guiding the release of this information to the destination site (J. Adjei & Olesen, 2011). Effectively, the issuer of the information is prevented from tracking the time and destination of information and its use and the destination site is equally prevented from linking users.

Identity Mixer (idemix) – IDEMIX which was developed by IBM Research and its partners is an anonymous credential system that enables strong identity authentication and information privacy. IDEMIX seek to guarantee information privacy by solving the privacy dilemma and thus, facilitating effective secondary uses of personal identity information within the identity life cycle Figure 8 by identity service providers and relying parties without trust erosion. IDEMIX emulates the concepts of Privacy by Design (Cavoukian, 2012) due to its ability to ensure minimum disclosure and ensuring that sensitive information is not revealed. This attributes of IDEMIX help in masking sensitive personal information in online transactions and thus fulfilling the principle of data minimization in the the seven laws of identity (Kim Cam-

eron, 2005; Cavoukian & Carter, 2006). Although credentials are fundamental concepts in IDEMIX implementation, it seeks to address the lapses in traditional face to face presentation of Identity credentials such as passports and driving license which could result in the disclosure of other vital information to third parties by virtue of such information being on the credential. IDEMIX in essence, focus on the object of credentials as providing a means to establish a claimed identity, roles, or attributes about an individual with an entity which is usually a critical part of access-control policies. IDEMIX based identity credentials thus provide a means of establishing the age or age predicate of a person without revealing the actual date of birth or age of that person. In essence such anonymous credentials, provides users the flexibility of selectively revealing on aspects of their identity attributes required in a transaction or a predicate of which making it possible to avoid wholesale disclosure of personal information. IDEMIX thus largely removes the possibility of linking users identity attributes by identity providers and relying parties. IDEMIX users initially obtain anonymous digital credential or voucher indicating the information the issuer is prepared to reveal from a trusted third party such as a bank, insurance company, or government agency. Subsequently users can authenticate themselves with service providers by issuing a claim or a statement using IDEMIX to securely transform the issued credential. Such transformed credentials will only contain the subset of the attested information that the user is willing to disclose. Although IDEMIX users can apply this transformation on many instances, none of the credentials can linked.

IDEMIX in effect, seeks to limit the need for undue disclosure of personal details in online transactions such as downloading music and movies or subscribing to online newsletters. In such transactions users leave traces and pieces of information such as size, frequency, and source of online purchases that can be traced back to the user. IDEMIX applications seeks to eliminate such trails with an artificial identity information, known as pseudonyms, making user online transactions anonymous. IDEMIX thus can allow users to transact without revealing their payment information which can easily be used in predicting users spending habits or provide proof of age without disclosing users actual date of birth. IDEMIX based systems in effect provide the technology for protecting users privacy by sharing only pseudonyms, so that real identity information can never be intercepted or exposed (Camenisch, 2012; Camenisch et al., 2011).

OpenID – OpenID is an open standard that describes the means by which users can achieve a decentralized authentication which eliminate the undue reliance on service providers for authentication. Thus the application of OpenID allows users to consolidate their digital identities by creating accounts with their preferred OpenID identity providers, and then use those ac-

counts as the basis for signing on to any website that OpenID authentications (Recordon & Reed, 2006). In effect OpenID standard provides a digital communication framework between the identity provider and the OpenID acceptor (the "relying party") to ensure privacy and information security OpenID Attribute Exchange provides a means of transferring user attributes, (i.e. Name and gender) from the OpenID identity provider to the relying party (Hardt, Bufu, & Hoyt, 2007; Recordon & Reed, 2006). This means that the OpenID protocol does not rely on a central authority to neither does it require a specific means by which to authenticate users. Thus, OpenID allows various forms of authentications including passwords, smart cards and biometrics. Organisations such as Google, Yahoo!, Facebook, PayPal, BBC, AOL, MySpace, IBM, VeriSign, etc., provides various variations of OpenID authentication solutions (Eldon, 2009).

Open Authorisation (OAuth) – OAuth is an open standard for data authorization that make it possible for users to grant limited access (either in scope and in duration) to third-parties to access their resources without sharing their passwords (P. J. Connolly, 2010; Hammer-Lahav, 2009; Mangiuc, 2012). In that way OAuth users are able to share their private resources (e.g., photos, videos, contact lists, bank accounts) stored on a particular location with another website although their credentials like username and password are not disclosed. Effectively the underlining philosophy of OAuth is similar to the valet key metaphor of cars. Thus, third parties can only have controlled or limited access to the car [40]. To make a scheme like the valet key metaphor possible, websites are given only the minimum information required to accomplish the task that user has requested. In effect it afford users the ability to to hand out to third parties tokens (instead of credentials) to their data hosted by a given service provider. Such tokens might include granting print *access* to photos without sharing username and password. OAuth 2.0 also provide specific authorization flows for internat and desktop applications, mobile phones, and internet of things (P. J. Connolly, 2010; Hammer-Lahav, 2009; Mangiuc, 2012).

Touch2id – Touch2id is a biometric and Near Field Communication (NFC) technology based identity verification technology which apply the concepts of minimum disclosure and data minimization principles in making the application user-centric and privacy-enhancing (Touch2ID, 2012). Touch2id is currently in use in certain parts of the United Kingdom to provide identity verification services, such as proof–of–age for young adults in public places using NFC service or mobile phone ‘sticker’. The application of data minimisation and minimum disclosure principles implies that the identity verification technology does not need to store the personal information of users such as name, date–of–birth, gender or address. Thus,

the technology can function efficiently without the need for central database as is the case of many identity management systems. Similarly it does not capture and store a fingerprint at enrolment or during authentication since it uses fingerprint sensor instead of a picture to confirm the claim that a person is 18 or over. In essence, Touch2id provides a form of zero–knowledge proof for the claim that an individual assert (i.e. I am over 18) since it does not reveal anything other than the veracity of that claim. Hence the relying party (i.e. a bar attendant) can check the identity of a potential customer with sufficient level of assurance without having (or needing) to know the individual's personal information and without generating an archival record of who visited which bars when. Touch2ID technology achieve this feat by harnessing multi–spectral fingerprint sensors that is capable of reading various fingerprints thus addressing common performance failures due to dirty or damaged fingerprints) and the emerging use of contactless smart–card technology, and NFC–enabled smart phones. In effect the applications non reliance on database for storing unique code created from the fingerprint, using a process known as minutiae mapping where the fingerprint itself is never captured and the approach therefore minimises the risks of unrevokable biometrics (Ratha, Chikkerur, Connell, & Bolle, 2007; E. Whitley, 2013).

The major features of the technology include:

- No personally identifying information is released relying parties since no name, age or photo appears on (or is stored on) the card and hence users movements and transactions cannot be easily profiled by merchants (Kim Cameron, 2010).
- There is no central database assembled that contains the fingerprints of innocent people whilst the fingerprint templates on the cards are digitally signed and can't be tampered with
- The fingerprint template remains the property of the person with the fingerprint – there is no privacy issue or security honeypot and thus credentials cannot be shared with friends and family since their finger would not match the fingerprint template.
- Misplaced or stolen touch2id based credentials cannot be reused since it will not work any more thus able to eradicate fake Identity credentials.

2.2.6 Identity Assurance

Conducting efficient and effective commercial and government businesses thrives on the ability to demonstrate the identity of all transacting parties beyond their immediate circle of trust. Identity assurance is a user-centric concept that seeks to allow data subjects to prove or provide informational representation during a chain of events that can define who they are with-

out the need for them being physically present (Crosby, 2008a). It aims at user satisfaction and thus focus on providing visibility into how risks associated with identity information are being managed. Such identity management solutions often deal with the storage, processing, disclosure and disposal of users' identities, their profiles and related sensitive information.

To ensure user satisfaction, identity assurance must be a key of an element of IdMS since it offers mutual benefits to identity providers and service providers, and to citizens. An identity assurance scheme can address issues such as the amount and type of data stored and the degree to which this information is shared. In identity assurance systems, the context and the nature of events define what prove or informational representation will be necessary and the kind of entitlement. For instance, clients of health insurance agencies might need to prove their status as unemployed, retired, etc.

Protection of personal data integrity is a major concern for all customers although, they may vary in their demand for privacy protection. Identity assurance schemes must therefore provide the options that will enable data subjects to make such informed choices. Identity assurance therefore differs from Identity management, in the sense that IdMs are primarily designed in the interest of the identity provider whereas identity assurance focuses on bringing benefits to the data subject. Yet the technology employed to achieve Identity assurance and management may be similar.

Kantara Initiative, a collaborative research organization focuses on requirement gathering for the development and operation of Trust Frameworks as well as verification of actors within Trust Framework ecosystems aiming at identity assurance schemes. **Error! Reference source not found.** illustrates identity assurance protocol, the insurance and its client both have a broker they can trust. The identity of the client is also assured, given that they do not need to reveal sensitive information to the service provider.

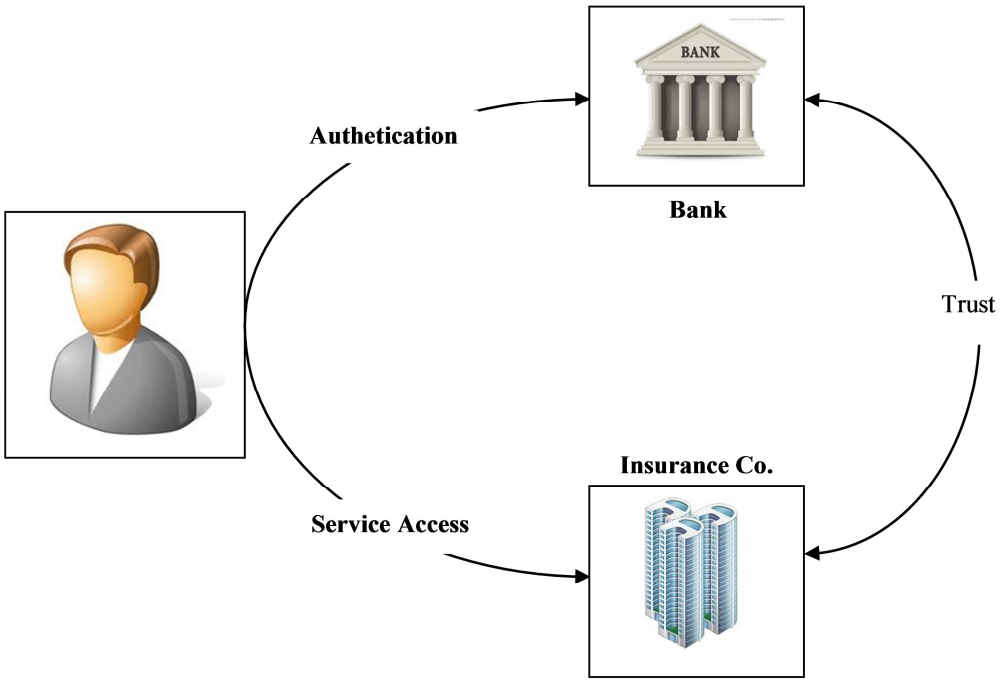


Figure 14 Typical Trust Framework.

2.3 Citizen[19] (National) Identification Systems

Governments in many countries implement IdMS as a means of establishing a reliable database of citizens and residents of the country. An efficient citizens identification system should assist government agencies in the provision of targeted services, improving governance and collection of taxes.

Technically, such citizen (national) identification systems follows the concept of trust management systems (Blaze et al. 2003) and might usually have a central database and 'identity cards' that are issued to citizens. The variations are usually in relation to the location and content of the databases, and the underlying technology (e.g. Smart card or biometrics), the communication architecture, etc. In such systems, credentials issued to citizens give them the right to access services.

Thus the overarching objective of many citizen identification systems is to improve the assurance of citizen's identity in their dealings with government agencies (Cofta, 2008). In effect, national identification systems unduly focus on the credential issuer and thus have negative implications on citizens' trust, due to its equation of secrecy to privacy protection. However, the undue focus on citizens' interactions with the state sometimes diminishes the benefits that

[19] The term 'citizen' refers to all individuals who can participate in the system, such as legal definition of citizens and all indivduals who have lawful residents status, refugees, etc.

could be derived from the system, and particularly discounting the rich experiences that citizens already enjoy with their identities on the internet. For instance, many of such systems fail to cater for group identity or the identity of anyone other than the individual (Cofta, 2008).

Furthermore, many countries also differ in their ability to realize the potential social benefits of a citizen identification system, including efficiency improvement in service delivery, reduction in cost of doing business, effective border control and improved government to citizen interaction, due to the risks associated with improper design or operation. Violation of citizens' privacy and other personal rights is due to intentional information sharing by those in possession of such sensitive information or by direct attack on the system making such systems a risky proposition from an information security perspective (D. J. Solove, 2002). This is part of the objective of the study, by highlighting the key issues needed to be addressed in order to make such systems effective.

2.4. Privacy and Personal identity information

Personal information is has become central to the business models of the digital age; admnistring government services and; and in citizens interactions. Various strategies are adopted by business organizations in personalising service delivery to customers, using customer preferences (Alatalo & Siponen, 2001; Norberg, Horne, & Horne, 2007; X. Wang & Xue, 2012). Although such practices offer customers convenience and personalized services, which can contribute to repeat purchases, it inherently requires collection of pieces of customers' personal data or attributes. Thus, the need for a critical look at what constitutes personal identity information (Andrade, Kaltcheva, & Weitz, 2002).

Any information that can specifically identify an individual (e.g. name, telephone number, e-mail address, or account number) is described as personal identity information. It can also include a person's location or activities like accessing a website. In his Onion Model (Wilton, 2008a), Wilton has illustrated this using his the layers of an onion to categorise personal information into three layers. These include the core, inner layer and the outer layer. Thus, information that can uniquely identify an individual and does not change over time, (e.g. Name, date of birth) was placed at the core. Information at the core is known as a Basic Identifier Set (Wilton, 2008a). The inner layer consists of information that is capable of being used for identification but susceptible to change over time, such as address, height, etc. The outer layer consists of information that cannot uniquely identify a person, except when combined with any other information or aggregated over time, such as a person's transaction history and sector specific information like blood group and health status. In effect, personal information is

any information describing a natural person or information that describes an identifiable individual (Trubow, 1992).

2.4.1. Secondary uses of Personal Information

Information must generally be used for the purpose of protecting, promoting, or meeting the physical needs of an individual or to enable that individual to participate in social interactions or benefit from services. Such information usages are regarded as the primary purposes of collecting personal information. For instance, the primary purpose of a Voter ID card is for an individual to vote in an election and that of a passport is to facilitate border control. Many of the data protection regulations mandate that personal information gathered for one purpose may not be used for any other purpose without the specific, informed consent of the data subject (Trubow, 1992). However, in order to conduct business such as opening a bank account, banks sometimes require tokens like a passport as a proof of identity. Such a requirement by the bank is secondary to the original intention of passports and voter IDs.

Secondary uses of personal information was conceptualised in Culnan (1993) as having two dimensions: (1) The information processing activity (acquisition, use, or transfer), and (2) The relationship between the consumer and the firm utilizing the information (existing customer or prospect) (M. J. Culnan & Armstrong, 1999; M. Culnan, 1993). Thus, secondary uses of personal information refers to the collection and storage of information for purposes other than originally intended by the issuer of the credential, whether legitimate or otherwise. Obtaining access to and enventual uses of personal information in principle results in a number of complex challenges. In essence, the legitimacy of secondary use of personal information hinges on an "implied social contract" (tacit or explicit consent by service providers to protect the interest of data subjects) between service providers and users (Milne & Gordon, 1993).

Perceptions of abuses of personal identity information perception results in issues of privacy and confidentiality, with it attendant effect on the trusting relationship that should exist between service providers and data subjects (D. Solove, 2006, 2013). Such perceptions and their effects are amplified by that technologies that make such abuses and breaches difficult to notice, and thus posing technological, policy and regulatory concerns in relation with the ability to collect, store, aggregate, link, and transmit personal information for legitimate purposes. Such challenges have generally been researched in information systems under information privacy.

2.4.2 Information Privacy Concerns

The concept of privacy has been studied in many different ways, given that it has many dimensions (H. J. Smith, Dinev, & Xu, 2011; H. J. Smith, Milberg, & Burke, 1996). Privacy has been described as a condition or a state in which an individual can be more or less inaccessible to others, either in the spatial, psychological or informational plane (E. Whitley & Kanellopoulou, 2010a). In psychology literature privacy is described as the ability of individuals to control the terms under which personal information is acquired and used (Westin, 1967). Similarly privacy has been described in sociology literature as individuals' ability to independently dispose of their roles according to their right of self-determination, and then to have confidence that third parties respect the intended separation of their roles (Biskup & Brüggeman, 1988).

Clarke (1999) on the otherhand defined privacy as individual's personal space, and provided a four dimensional categorization of individuals' personal space as; *privacy of the person (concerned with the integrity of the Individual's body), privacy of personal behaviour, personal communications, and privacy of personal data (R. Clarke, 1999; Roger Clarke, 1999).*

Contemporary research have merged personal communication and data privacy into what is now referred to as information privacy, given the the increased digitalization of information and communications (France Bélanger & Crossler, 2011; Pavlou, 2011a). Hence, information privacy refers to the claims of individuals that their personal data should generally not be available to others, and that, where data are possessed by another party, the individual must be able to exercise a substantial degree of control over the data and their use (France Bélanger & Crossler, 2011)

Information privacy concerns are related to factors affecting a person's willingness to render personal information (Dinev, Xu, Smith, & Hart, 2012), engage in online transaction activity (Pavlou, Liang, & Xue, 2007), and the attitude towards government regulation (Milberg, Smith, & Burke, 2000). Although individuals express privacy concerns, many are willing to trade-in their privacy for convenience. This so-called privacy paradox (J. Adjei & Olesen, 2011; Norberg et al., 2007; D. Solove, 2013; Zallone, 2010) also reaffirms the need for a more measured treatment of personal information.

Thus, information privacy is not about secrecy, which is an intentional concealment of information and (or) a disposition towards the sharing of potentially inaccurate information (Trubow, 1992). OECD guidelines (OECD, 1980), and other national data protection laws address various aspects of information privacy concerns, such as; (1) The existence of record systems cannot be kept secret; (2) an individual must be able to "find out what information

about him is in a record and how it is used"; and (3) an individual must be able to "correct or amend a record of personally identifiable information (D. Solove, 2006).

(France Bélanger & Crossler, 2011) observed that development of privacy tools and technologies is usually done in isolation of the actual users and for that matter, their input is not reflected in the systems design. The research approach adopted in this study is to address such concerns and to ensure active user involvement in secondary uses of their personal information.

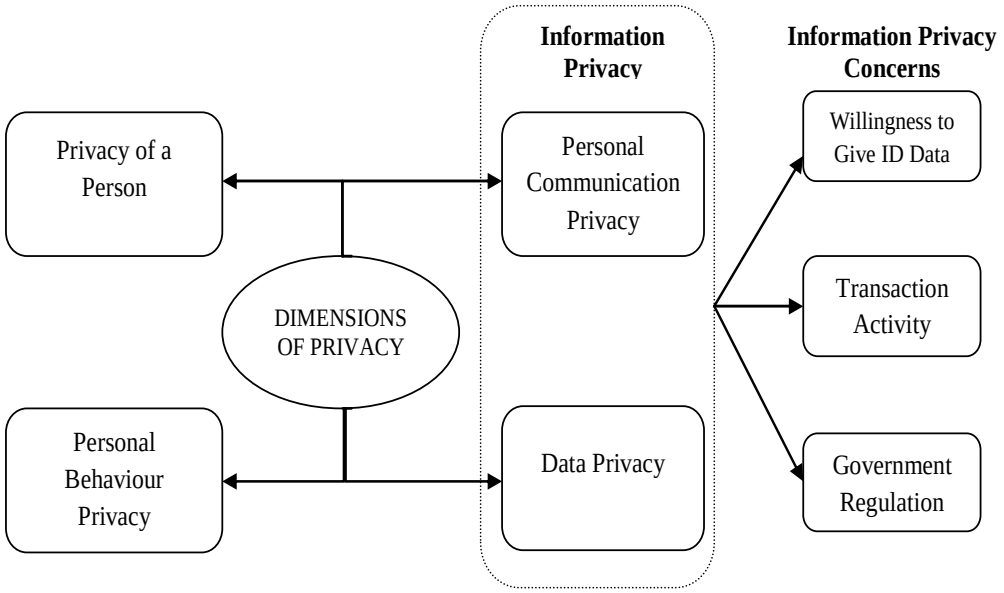


Figure 15 Dimensions of Privacy

Figure 15 outlines the dimensions of privacy. Information privacy concerns issues of personal communication privacy and data privacy. Such concerns emanates from and are associated with data collection, data processing and data dissemination. Information privacy concerns therefore can influence and affect individuals' willingness to provide information, their transaction activities and responses to the identity policies of government agencies.

2.5 The Concept of Trust

> Three things are needed for government: weapons, food, and trust. If a ruler can't hold on to all three, he should give up weapons and food and hold on to trust: "without trust we cannot stand" Confucius.

Historically, human beings have lived in smaller communities and close-knit societies and have had the confidence assurance that the name of a member identifies him in the community. In such communities there were not many information secrecy and thus, a person's name carried a great deal of information. Interestingly, in contemporary society, we interact with people (entities) that we barely know and sometimes might never meet. Such a phenomenon has brought the concept of trust to its current pole position in identity management discus-

sions. Thus, failure to do such due diligence can result in serious business and social implications.

The concept of trust has been studied from different perspectives such as sociology, psychology, economics and political sciences but a willingness to take risks may be one of the few characteristics common to all trust situations (Heavey & Murphy, 2012; Johnson-George & Swap, 1982; R. C. Mayer, Davis, & Schoorman, 1995). In the context of personal identity information use, parties are expected to act and react willingly. In essence, trust is a firm belief in *a firm belief in the reliability, honesty, veracity, justice, good faith, in the intent of another party to conduct a deal, transaction, pledge, contract, etc. in accordance with agreed principles, rules, laws, expectations, undertakings, etc* (Slone, 2004).

Trust is not transitive (cannot be passed from person to person); distributive (cannot be shared); associative (cannot be linked to another trust or added together); symmetric (I trust 'you' does not equal 'you trust me'); self-declared (trust me – why?)

This is in line with the definition of trust as "the willingness of a party to be vulnerable to the actions of another party, based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (R. C. Mayer et al., 1995). This presupposes that in the identity management process, data subjects are perceived to be in a vulnerable position and trust is what will induce parties to engage in transactions irrespective of the vulnerability levels. Thus, trust is the probability that a party to a transaction will act in a way that is beneficial or at least not detrimental to the interest of the other party for the latter to cooperate (Gambetta, 2000). The above definitions make the differences between predictability and trust unclear and hence the need to situate trust in its proper context. Although the two are a means of reducing uncertainty, trust goes beyond predictability and hence reduction of uncertainties. Otherwise, those who can consistently ignore the desires and intentions of trustors and act in their own self-interest can be deemed to be trusted, because of their predictability (R. C. Mayer et al., 1995).

2.5.1 Trustworthiness

The relationships between the actors in trusting in trusting relationships is a major source of reference in explaining the concept of Trustworthiness. The key actors in trusting relationships include the; trustor, trustee and context (Kramer, 1999). *Trustors* in the context of this study includes citizens (or virtual citizens, since trust can also be a matter between virtual persons (Cofta, 2008). On the otherhand *trustees* are the credential issuers and relying parties and the *context* is the identification scheme. Trustworthiness is based on the attributes exhibited by the trustees within the context. Mayer et al, (1995) identified three important charac-

teristics that help in building the foundation for the development of a trust framework (R. C. Mayer et al., 1995). Ability, integrity and benevolence have been identified as the key characteristics of trustees in the trust development process. Ability signifies competences, perceived expertise, business acumen and judgement that enable the trustee to have influence within a particular domain. Benevolence on the other hand connotes the extent to which the trustee can be assured of going beyond the profit motive to serve the interest of the trustor.

Essentially, benevolence suggests that the trustee will behave in a desirable manner towards a set objective, irrespective of their personal preferences (Rosen & Jerdee, 1977). Integrity is premised on the trustor having a positive perception that the trustee will adhere to a set of acceptable principles. Thus adherence to a set of moral principles accepted by the trustor defines personal integrity. The concept of trust and trustworthiness thus has multidimensional constructs of ability, integrity and benevolence. Ability is characterised by competence or perceived expertise; integrity signifying consistency, fairness and reliability; whereas loyalty, openness and availability describe benevolence (J. Adjei & Olesen, 2011; R. C. Mayer et al., 1995). Therefore a trust relationship can be negatively affected when the trustee consistently provides wrong information, refuses to provide or delays in the delivery of personal information to a legitimate recipient, or provides legitimate information to the wrong persons. Hence, users' perception of trust towards an identity management system (IdMS) is an important determinant of its success as they can affect the usage behaviour of the systems.

2.5.2 Dimensions of Citizens' Trust

Using Hattori & Lapidus (2004) concepts of trust relationships, Srivastava & Teo, (2008) created a trust grid to model the level of citizens' trust in e-government technology (Hattori & Lapidus, 2004; Teo, Srivastava, & Jiang, 2008). We have adapted the framework for accessing the role of trust in IdMS success. Perception of trust can be either due to the technology or the institutions (S. C. Srivastava & Teo, 2009; Teo et al., 2008). A low citizens' trust in credential issuers and a low citizen's trust in IdMS will be a major disincentive to accept the IdMS since there is a lack of identity assurance (Crosby, 2008a). Such lack of trust on both dimensions can lead to unfavourable outcomes which are not suitable for the success of the IdMS. Likewise, a low trust in credential issuers coupled with a high trust in the technology leads to a situation where citizens might use technology as a competitive tool against the unpredictable and sporadic results. In such a scenario, the IdMS will be viewed with suspicion and cynicism by the citizens (S. C. Srivastava & Teo, 2009; Teo et al., 2008).

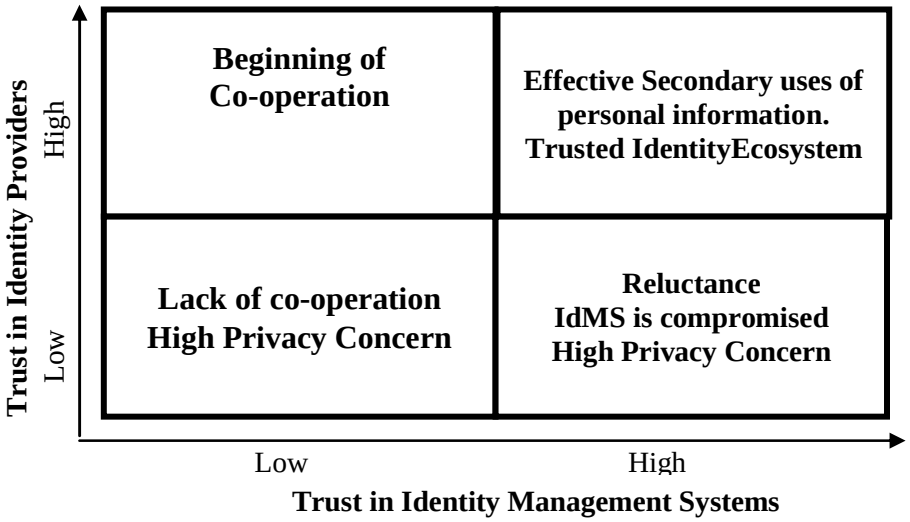


Figure 16 Dimensions of Trust (Hattori & Lapidus, 2004; Teo, Srivastava, & Jiang, 2008a).

A low level of citizens' trust in IdMS, coupled with a low level of trust in credential issuers could breed distrust in the identity ecosystem leading to suspicion and cynicism. Similarly, a low level of trust in credential issuers and a high level of trust in IdMS can lead to a situation where the patronage of the IdMS is merely a means of positive defiance.

When the identity issuer is trustworthy, citizens begin to cooperate even when trust in IdMS is low. A high level of trust in credential issuer coupled with a high level of trust in IdMS will result in synergy between the government agency and citizens. Citizens begin to feel that their identity is assured in transactions involving exchange of personal information. It also encourages institutional cooperation, effective secondary uses of personal identity information, interoperability. This is the desired conditions for trusted identity ecosystem.

2.6. The Identity Ecosystem in Ghana

An Identity Ecosystem is an environment where individuals, businesses, and other organizations enjoy greater trust, privacy and security, as they conduct sensitive transactions and interactions (Grant, 2011a). It is thus a user-centric identity environment governed by a set of technologies, policies, and agreed upon standards that securely supports transactions ranging from anonymous to fully authenticated and from low to high value transactions (Bertino, 2012; Grant, 2011a).

In Ghana, several IDMS have been implemented with various forms of credentials issued to citizens. The major credential issuers as in Figure 17 include; National Identification Cards, Birth Certificates, National Health Insurance Cards, Biometric Passports, Biometric Driver's Licenses, Biometric Voter's Identity Cards and Tax Identification Numbers (TIN) are some of

the widely used credentials. The birth certificate which should be the primary source document for acquiring identity credentials has many challenges. Currently, the civil registration coverage in Ghana is 71% based on UNICEF 2012 statistics (UNICEF, 2012) implying that out of the population of 24.66 million (UNICEF, 2012), 29% (7.15 million) are not registered. Besides, there are other challenges with respect to the registration system, ranging from multiple registration, multiple name changes, etc.

Existing IDMSs are all in silos and each of the existing IdMS are primarily used by the credential issuers as a means of fulfilling their functions. Many of the citizens' registrations are unduly influenced politically, resulting in the recruitment of unqualified personnel and its effect on trust.

The technology being used to manage identity comprises of manual systems, computerised systems and different variations of biometric technology. All the identification systems are for face to face verification and thus Internet applications of IdMSs are not given the requisite attention. Many of the commercial banks in Ghana issues various customised cards and visa cards to their customers that is used for ATM withdrawals and various forms of electronic banking transactions. Currently, none of such credentials can be used for proof of identity, although customers have a comparatively high level trust in the financial institutions.

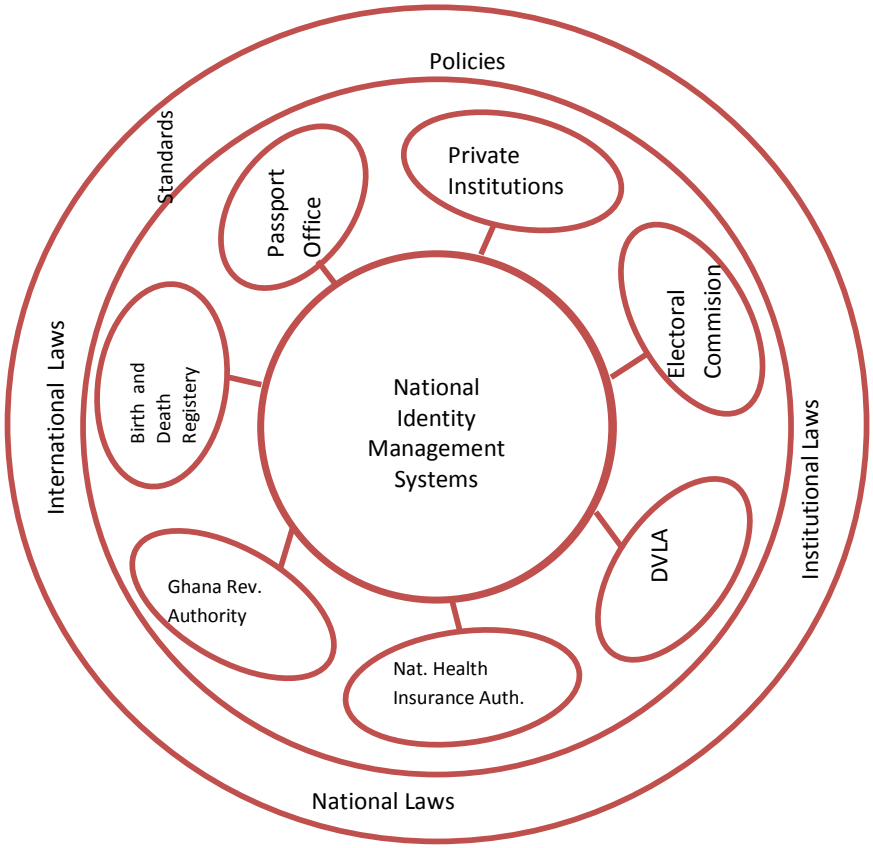


Figure 17 Institutions that Issue Credentials in Ghana.

Changes to citizens' personal data is handled by each of the credential issuers independently. Thus, service providers have no legal process of verifying and authenticating credentials in real-time via the internet or mobile platforms. This hinders the effective uses of the systems beyond the primary purposes. In spite of its use being lower than expected, identity management can play a central role, if the factors that affect its takeoff are properly addressed as is evidenced in recent statistics in Europe.

This next section provides an overview of civil registration system, voter identification system and the National Identification Card. Passports, drivers' license, and other credentials issued by government agencies and private institutions are not discussed in detail. In the case of passports and drivers' licenses, although they are some of the generally accepted credentials for proofs of identity, the information in Table 4 indicates their limited circulation, given that majority of Ghanaian residents do have drivers license and passports. Similarly, tax identification number (TIN) and social security cards are not commonly used for either authentication or identity verifications beside their primary use.

TYPE OF IDMS/CREDENTIAL	NATURE OF CREDENTIAL	LEGAL REQUIREMENTS
National Health Insurance Card	Plastic Card, valid for 5 years and renewable every year. Accepted for proof of identity	Optional
Voters Identity Card	Biometric database and laminated paper card. Accepted for proof of identity	Mandatory for all voters.
Passport	Biometric based passport. Accepted for proof of identity.	Mandatory for international travel
Drivers License	Biometric database and a Plastic Card, valid for 6 years and renewable every 2 years. Accepted for proof of identity	Mandatory for all drivers
National Identity Card	Biometric database. Plastic card based on 2 dimensional bar code. Many of the cards not yet issued	Mandatory for all citizens and residents
Social Security Card	Laminated paper card. Not accepted for proof of identity	Mandatory for all employees
Tax Identification Number (TIN)	The TIN is issued by the Ghana Revenue Authority to registered businesses and employees. No credential is issued.	Mandatory for businesses and the employed
Birth Certificates	Paper based form. Used as proof of identity for acquisition of other credentials.	Issued at birth or when a person registers
Baptismal Certificates	Paper based card issued by churches. Sometimes used for proof of identity for acquisition of other credentials.	Optional
Credentials Issued by banks and educational institutions	Visa/Master/proprietary cards (e.g. Students identity card). Not accepted for proofs of identity	Optional

Table 4 Types of Credentials in Ghana.

2.6.1. Civil Registration in Ghana

Vital registration in Ghana began in 1888 when the earliest known vital registration law, the cemetery ordinance was passed. This law was then limited to the registration of deaths, mostly expatriate workers of the then colonial government. It was not until 1912 that the registration of births was introduced. The civil registration system has gone through a series of transformation with the aim of improving the system and widening the coverage. For instance, the cemetery ordinance of 1888, was then amended in 1891 and in 1912, at which time it became Births, Deaths and Burials Ordinance. The law was amended again in 1926 until it was finally replaced with the Registration of Births and Deaths Act 301 of 1965, which is the legislation currently in force.

The Births and Deaths Registry is under the Ministry of Local Government and Rural Development, and is responsible for developing and managing the births and deaths registration system in Ghana. Its operations are co-ordinated from the Central Registry Office, in Accra, the capital of Ghana and operates in all local administrative districts each of which is manned by a District Registration Officer and a Registration Assistant.

The Registration Assistant submits monthly, all registration forms, numbered serially to the District Registration Office, which in turn forwards them to the Regional Office for further processing and onward transmission to the Central Registry Office, where national data is

compiled. Statistics of registered events are kept at all three levels. Presently, information in the CRS databases is not used by any of the other credential issuers for their operations.

2.6.2. Voter Identification Card

The Electoral Commission (EC) is the institution responsible for the management of elections in Ghana (GNA, 2003). The existing commission was established in 1993 by Act 451. It was set up purposely to manage the conduct of all public elections and to handle all matters directly relating to the conduct of elections in the country. Its functions include supervision of all public elections and referenda, compilation and revision of voter register; demarcation of electoral boundaries and provision of civic education concerning the electoral process.

Elections in Ghana are conducted using a manual system, whereby voting, counting and collation are all done manually. In the year 2012, the EC decided to implement biometric systems for voter registrations and identity verification during elections. A new voter register was compiled by capturing ten fingerprints and photos of all applicants resulting in the issue of a laminated paper based voter identity card.

Biometric verification devices were also procured for all the 25,000 polling centres across the country to be used on the Election Day. According to the chairman of the EC, the voting system remains manual and the biometric verification devices were only meant to check the identity of the voter by their fingerprint (Afari Gyan, 2012).

Although the nation invested USD82,326,497 on the biometric based registration (Table 5), it could not prevent the perennial issue of election disputes. Rather, it compounded the problem since for the first time in history of the existing dispensation, the first round of voting took two days. The main opposition did not accept the results of the presidential election and thus proceeded to the supreme court citing; multiple voting; over voting were 620,443; voting without verification 456,933; same serial numbers for different stations with total irregularities of 1,340,018 votes.

Such issues which are common phenomena in African elections (Bratton, 1998; Evrensel, 2010; GhanaReporters, 2012; McDermott, 2012) are indications of the growing perception of lack of trust in the institutions and also clear manifestations of the need to address the fundamental issues in citizen identity identification. Hence in developing countries, solution to identification issues does not lie in the acquisition of sophisticated technology since biometric voter registration (as is the case of many IT applications) only counters the symptoms without addressing the causes which is in this case electoral irregularities (Bhalla, 2012)

Year	Type of registration	Cost in US$	No of Applicants	Cost per Applicant in US$
2002	Revision	918,000	480,000	1.91
2004	Full registration	12,437,000	10,355,000	1.20
2006	Revision	2,430,000	632,000	3.85
2008	Revision	19,792,000	1,835,000	10.79
2012	Full Biometric Registration[20]	82,326,497.00	14,031,793	5.86

Table 5 Voter Registration Statistics.

2.6.3. National Identity Card (Ghana Card)

Citizens identification in Ghana began in 1972 during the administration of the second prime Minister through the implementation of the identity cards decree (NRCD129). This law required Ghanaian citizens aged sixteen years and above to be issued with identity cards which were to be accepted as evidence of the identity of the holder in cases where the identity of the holder is in dispute. Recruitment for all kinds of employment were to be based on the ability of the applicant to produce an identity card as evidence eligibility. Public and private employers would be required to enter the identity card number of each employee in the personal records of that employee, and each person responsible for social security scheme was to use the allocated identity number instead of the scheme number. In 1973, national identity cards were issued to citizens in five border regions of the country. The project was however discontinued three years later, due to lack of financial and logistical support.

In 1987, the government, through the then National Commission for Democracy, established a technical implementation committee, to examine and propose a unique numbering system, an appropriate computerised system, the cost involved, and the possible sources of funding. This project was again put on hold.

The government again decided in the year 2001 to develop a comprehensive biometric based national identification system. Act 655 was enacted to amend a section of the Electoral Commission Act of 1993 (Act 451) and to repeal the law that gave the commission the right to issue civil identities (GNA, 2003). This was replaced by the NIA law, ACT 707 to reflect the

[20] The actual cost of the biometric registration and provisional exhibition was GH¢156,420,344.00, which was converted to US dollars at an exchange rate of US$1.90

real position on the issuance of a national all-purpose identity card. It also generated a major debate in parliament on the necessity of setting up a new institution instead of allowing the Electoral commission to issue National Identity cards. The major contention was whether it was prudent in spending the budgeted 400 billion old cedis on a new institution or give the Electoral Commission the needed 100 billion old cedis for a new voter's registration. The EC was seen as an organisation with a secure tenure and credibility. The then government decided to establish a new organisation to undertake such an exercise whilst the Electoral Commission concentrated on elections. When the legislation enabling the compulsory gathering and storage of biometric data was finally pushed through Parliament in 2006, the decision was unanimous, with the government and the main opposition lauding the identity project as an 'important step forward' and 'crucial tool' of national development.

The decision was to give the contract to a company with the requisite experience and capacity to implement and then transfer a national infrastructure for identity registration to the government as a two-year project. The project entailed the design and development of a large Automated Fingerprint Identification System (AFIS) that will store fingerprint details submitted for authentication purposes. Citizens and residents' enrollment program were to be embarked on nationwide using a thousand mobile registration stations, a fingerprint and biographical data capturing equipment. Each participant was to be issued a card to be manufactured by a card manufacturing company in Ghana. The issued plastic cards would store encrypted fingerprint details of holders using two dimensional barcode.

The contract was awarded to Sagem, following a tendering process that saw Sagem, Hewlett-Packard/Printrak, NIKUV from Israel, Marpless a consortium from South Africa. After Sagem had been granted the tender, the officials at the National Identification Agency began to discuss the implementation of the new system with government departments and political constituencies. A major issue that confronted the officials was the state of the Births and Deaths Registry, the division responsible for producing the documents that Ghanaians need to prove their identities. The identity card campaign in collaboration with UNICEF, injected new urgency and significance into the infrastructure of vital registration in Ghana in 2004, resulting in an increase in civil registration coverage of from less than 30 to nearly 50 per cent of estimated births.

Another problem is in relation to the boundary line around their population: a workable test of citizenship in the context of fluid boundaries and centuries of migration. In Ghana's case, the issues were compounded by the large numbers of foreign nationals claiming dual citizenship. NIA's initial discussions with Births and Deaths Registry officials revealed that only a small

percentage of Ghanaian citizens had birth certificates that could be used to prove their citizenship. Thus, the need for alternative arrangements involving lawyers and political scientists to outline a clear definition of who a Ghanaian is.

In the end, the government relied on relatives and opinion leaders to vouch for those whose identity was in doubt (NIA, 2007). This resulted in long queues during the enrolment processes and thus, stringent checks were not carried out in many registration centres. In the national political debate about the introduction of the identity card, there was warm consensus between the two main political parties about the development and political benefits that would follow from the introduction of identity cards. Currently, the project has stalled again due to funding with many of the credentials not being issued to citizens.

Ghana Health Insurance Systems

In the year 2000, the then President Kuffour government set-up a ministerial health financing task force to design a national health insurance scheme. The work of the task force resulted in a legislation that was submitted to parliament for approval into law. After a lengthy debate, the then government had its way and the ensuing law, ACT (650) establishing Ghana's National Health Insurance Scheme was passed. A governing body, the National Health Insurance Authority was set up and tasked with the responsibility of implementing the national health insurance scheme. Three types of schemes were provided for; the District wide Mutual Health Insurance Scheme (DMHIS); the Private Mutual Health Insurance Scheme (PMHIS) and the Private Commercial Health Insurance Scheme (PCHIS). The DMHIS is a state-issued or sponsored health insurance program and receives subsidies from the government for payment of claims and reinsurance in case of distress. The major sources of funding include 2.5% VAT on goods and services or the health insurance levy; 2.5% SSNIT contribution of formal sector workers; the premium for informal sector workers, investments, donations, budgetary allocations, and other funding from donor partners. Every person residing in Ghana other than the Armed Forces of Ghana and the Ghana Police Service are required to register with a recognized health insurance scheme.

The cards issued to registered members are magnetic stripe cards carrying a unique serial number which in future could be verified by the system during user authentication. The cards have the following security features; NHIS hologram, Picture-in-picture; and a watermark of NHIS logo and Ghana Coat of Arms. It also shows the picture of the bearer on a white background.

Membership is subject to yearly renewal according to the dates at the back of the card. A security sticker is affixed onto the appropriate slot each year when membership is renewed. A

card can be replaced before the five (5) year validity period if lost or damaged, at a fee. Currently, there are 13,943,414 card bearing members, representing 59.50% of the country's population (NHIS, 2010).

2.7. The Danish Civil Registration System

Denmark is rated among the front-runners Information Society development and has been ranked among the top 10 members of OECD country performance statistics in internet penetration and standard of living. Nationwide registration of people residing in Denmark started in 1924 with the manual registration on index cards information concerning members of each Danish family. This was followed by regular continuous update of the index cards database by local and municipal registration offices commonly referred to as Borger Service. The manual database was replaced in 1968 with an electronic version called Danish Civil Registration System (CRS). A detailed description of CRS has been published previously (C. B. Pedersen, Gøtzsche, Møller, & Mortensen, 2006; C. B. Pedersen, 2011). Individuals living in Denmark were registered for administrative purposes like collection of taxes and filing of tax returns by Danish residents. All newborn babies and those who have been given permanent residential status were also registered. The civil registration was extended to include those living in Greenland in 1972. The Danish civil registration system contains about 8,284,477 of which 65.8% of the population are estimated to be living in Denmark and 26.6% not alive. (C. B. Pedersen et al., 2006; C. B. Pedersen, 2011). The systems also give clear indication of all Danish residents living abroad. Thus due to the continuous update of the register, there is a clear indication of persons alive and resident in Denmark, (including Greenland), and those who are dead and the dates of their occurence. Those whose residence status is in doubt are also known to the Danish authorities.

In Denmark, all registered persons in the central registration system are assigned a "Centrale Person Register" (CPR) number which is a unique personal identification number. The CPR number is used in all interactions with government agencies and many business transactions and thus allows accurate linkage between all national registers. The Danish CPR-number is made up of 10 digit code with a logic built into it. For instance, a person's date of birth is used as the first six characters or digits presented in day of birth, month and year of birth (i.e. DDMMYY). The following three characters (character positions 7,8,9) are serial number to distinguish between persons born on the same day (Malig, 1996; C. B. Pedersen, 2011). The last four characters is also an indication of the century within which a person is born. For instance the 7th to 10th digit is less than 5000, it means the person was born in this century, else the person was born in the previous century (Malig, 1996). The tenth digit indicates the gen-

der of the person, with odd numbers indicating a male and an even number indicating a female. The tenth number is also used as a control check to minimise recording errors (Malig, 1996; C. B. Pedersen, 2011).

Thus, a female born on 16th June 1971 will have a CPR number similar to 160671-4362. The same principles are followed in the case of persons who were not born in Denmark, but arrived from another country. Every new entrant from other countries must register at central registry or the Borger Service and are issued with a CPR number following the same logic. On few occasions where individuals have been assigned an incorrect number (i.e. wrong date of birth or gender), a new CPR number is issued to the person and the previous number is never reassigned. Another interesting aspect of the Danish CRS is its ability to clearly establish a clear parental linkage of a person based on the legal relationship. In the Danish CRS systems, there is no ambiguity about the identity of a person and thus no possibility for confusion where two or more people share a similar identity attributes, making it possible for public authorities to administer precise rules concerning citizens. This includes payment of the right amount of social security benefits, etc., to the right person and likewise collection of the right amount of taxes. This level of accuracy makes the CRS vital to government to citizens interactions once the major privacy concerns are addressed (Blume, 1989; Malig, 1996; C. B. Pedersen, 2011).

Single identification number

In Denmark, all residents have a single identification number. The CPR number is issued by the Danish Ministry of the Interior to every Danish citizen, and other ordinary residents who have the right to remain in the country. All public authorities and organisations can use the system for unequivocal identification of a person or as a file number, which is a common practice.

However, information on the CPR may be passed on to another public authority only if it is allowed under the Danish Processing of Personal Data Act. Private persons may use the number mainly if they are entitled by law or by regulations laid down by law, with the consent of the registered person or if it is to be used solely for scientific or statistical purposes.

The CPR number also takes precedent over all other document numbers and thus many of the important credentials also bears the holder's CPR number. The National identity cards, Passports, Social security or health insurance cards, Driving licenses, Tax statements and notifications, documents for enrolling children in school or at the university, Bank Accounts, etc., are all official credentials and documents bearing the CPR number as shown in Figure 18.

Compared to Sweden and Finland, two other Scandinavian countries, the Danish CPR numbers are widely used. In Ghana however, none of the official documents display the birth certificate number.

Documents and Credential	Country			
	Denmark	Sweden	Finland	Ghana
National identity cards	√	√	√	N/A
Passports	√	√	√	N/A
Social security or health insurance cards	√		√	N/A
Driving license	√	√	√	N/A
Tax statements and notifications	√	√	√	N/A
Voter Register (Voter ID)	√	√	√	N/A
Documents for enrolling children in school or at university	√	√	√	N/A
Other – e.g. Bank Accounts	√			N/A

Figure 18 Documents Bearing the Unique Identification Number.

Chapter 3 Theoretical Perspectives

An overview of identity, identification, the state-of-the-art on IdM and of trust, privacy and information privacy was presented in Chapter 2. The contextual issues were also presented in Chapter 2 by highlighting the existing IdM issues. It is this background that set the stage for analysis of related literature that predict, describe or explain cutting-edge privacy-enhancing IDMS proposals. Thus it seems appropriate in this chapter, to examine the theories and research perspectives in relation to successful implementation of trusted identity management systems. The selection of literature was based on the materials' usefulness to understanding of or critique of existing beliefs, central to shaping knowledge of the phenomena, the research objective and the related research questions as defined in various sections in Chapter 1. Such initial understanding fomented an intentionally constructed theoretical basis of the research phenomenon, and also acted as a frame of reference for my research methodology.

3.1 The Streams of Research

The theoretical underpinning of this study draws from multivariate sources, given that the concepts of identity and identity management have different domains of relevance. The selection of relevant scholarly literatures was based on its orientations towards information systems success, and stakeholder analysis. This crosscutting perspective seems natural in a national identity management research and it is also in line with Weiser's concept of *"cycle of cross-disciplinary fertilisation and learning*[21]*"* (Weiser, 1993).

This study takes the position that although some measures of system's effectiveness (ease of use, usefulness, relative advantage, etc.) are commonly used, it is important to recognise the contextual factors. This view is in line with Sarker and Wells, (2003) position that merely instantiating existing theories in a new context, could potentially ignore unique issues associated with the context (Sarker & Wells, 2003). We therefore offer a framework that seeks to integrate the contextual issues associated with trusted identities environment especially in developing countries.

[21] We can make much progress both in evaluating our technologies and in choosing our next steps. A key part of this evaluation is using the analysis of psychologist, antropolisgist, application writers, artist, marketers and customers. We believe they will find some features work well and know they will find some features do not work. Thus we will begin again in the cycle of cross disciplinary fertilization and learning.

3.1.1 IS Success in Context

Information Systems have significantly changed governance and the cost of doing business since the inception of commercial computers in the early 1950's. Such developments have been attributed to the increasing power of computer systems and the comparable reduction in cost due to the Moore's Law effect (Schaller, 1997). Such growing complexity of information systems can also be seen in the growing complexity of the evaluation of its effectiveness or success (Petter et al., 2012). Perhaps there is the need to draw from information systems, success literature to find answers to such questions. Several quantitative and financial based models for measuring Information Systems (IS) success has been proposed (Delone & McLean, 2003; Petter et al., 2008). Other non-financial factors are also known to contribute to IS success (Kaplan & Duchon, 1988). Petter et al. (Petter et al., 2008, 2012) qualitatively examined IS success at both individual and organizational levels of analysis and found the D&M IS success model a useful instrument for measuring IS success both at the individual and organizational levels of analysis. They however posited that some of the dimensions may no longer be relevant or may need to be measured differently from other types of IS. In their analysis, they also observed that IS success or performance measurement has seen little improvement over the past decade with the tendency of researchers focusing on single dimensions of IS success instead of showing the overall picture. They further contended that valid and reliable measures have yet to be developed, although they admitted that the model is still relevant to contemporary IS success measurement. However, researchers must take a step further and apply rigorous success measurement methods to create comprehensive, replicable, and informative measures of IS success.

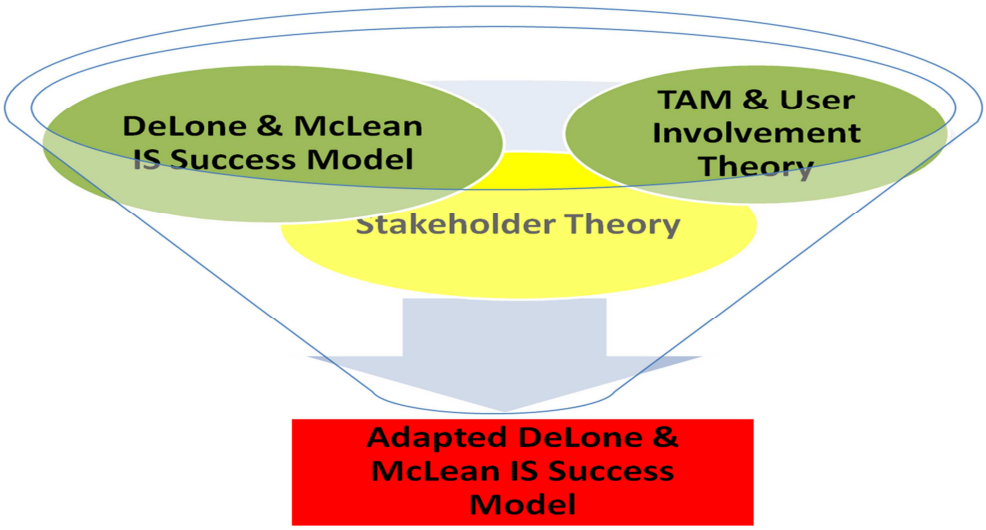


Figure 19 Summary of Theoretical Perspectives.

3.1.2 Technology Acceptance Model

Factors affecting technology adoption have been extensively studied in Information Systems literature. Technology adoption models have traditionally attempted to predict technology usage. (Morris & Dillon, 1997) posits that user acceptance is “the demonstrable willingness within a user group to employ information technology for the tasks it is designed to support”. Notable research on adoption and diffusion of technology includes Innovation Diffusion Theory (Rogers, 1983), TAM (F. D. Davis, 1989) and the unified theory of acceptance and use of technology (UTAUT) (Viswanath Venkatesh, Morris, Davis, & Davis, 2003). In (F. D. Davis, 1989), perceived usefulness and perceived ease of use were theorized to be fundamental determinants of behavioural intentions to accept or reject information technology. Perceived usefulness essentially describes the degree to which a person believes that an innovation will boost their performance (F. D. Davis, Bagozzi, & Warshaw, 1989) Perceived ease of use on the other hand describes the degree to which a person believes that adopting an innovation will be free of effort. In effect, users are more likely to adopt systems, which are easier to use and offer some benefits, since these two factors can affect the behavioural intention to consider using it and actually using the innovation. This theory is therefore relevant to the study of trusted IDMS.

3.1.3 User Involvement in IS Success (Blake Ives & Olson, 1984)

User involvement and user participation have often been used interchangeably, although the two terms do not have the same meaning and that the two should be clearly distinguished. Ives and Olson (Blake Ives & Olson, 1984) performed a five year review of IS success literature on the importance of user involvement in the development of information systems. Three levels of user involvements were identified; primary users of the system, secondary users and top management. Barki & Hartwick, (1989) have defined user participation as "a set of operations and activities performed by users" during system development and reserve the term user involvement for a "subjective psychological state" which influences user perceptions of the system and thus affects system success (H. Barki & Hartwick, 1989; Henri Barki & Hartwick, 1994). The working definition of user involvement in this study was *"the participation in the systems development process by representatives of the target user group"*. They also observed that studies on user involvement draw from research on organisational behavior, in which participatory decision is used extensively. Thus that active user involvement develops realistic expectations of the system, provides grounds for conflict resolution between the development team and the users, decreases user resistance, and increases system

ownership by the users, which, in turn, commits users to the system (Blake Ives & Olson, 1984). User participation in decision making in effect;

- Provides accurate requirements analysis (Cavaye, 1995; McKeen & Guimaraes, 1997; Robey & Farrow, 1982);
- Avoids unacceptable or unimportant features (McKeen & Guimaraes, 1997; Robey & Farrow, 1982);
- Improves user understanding and increases the tendency for users to own the system (Lucas Jr, 1974).

REFERENCES	EXISTING SUCCESS MEARSURES
(Blake Ives & Olson, 1984)	User performance, User satisfaction
(DeLone & McLean, 1992)	System quality, Information quality, System use, Individual impact, Organisational impact.
(Delone & McLean, 2003)	System Quality, Information quality, Service Quality, Intention to use, Use, User satisfaction, Net Benefits.
(Sabherwal, Jeyaraj, & Chowa, 2006)	**Context:** Senior management support, IS facilitating conditions, Quality of IS team **User related factors:** User IS experienced. User attitude, User participation **System success:** System quality, Perceived usefulness, User satisfaction, System usage

Table 6: Classifications of IS Success Measures.

3.1.4 DeLone & McLean IS Success Model (DeLone & McLean, 1992)

A number of models have been applied in the past to explain what constitute IS success. For instance Davis's (1989) Technology Acceptance Model (TAM) (F. D. Davis, 1989), the Theory of Reasoned Action (Ajzen & Fishbein, 1977; Fishbein & Ajzen, 1975) and Theory of Planned Behavior (Ajzen, 1991) have sought to explain the factors that make users accept Information systems. However in the study of the information system success, it has been established that technology acceptance is not equivalent to technology success or effectiveness, although it can be a necessary precondition to information systems success (Petter et al., 2008). Due to its complexity, and multi-dimensional nature of IS success, there were no precisely defined IS success constructs in the past. The original Delone & McLean IS Success Model was a major attempt to synthesize previous IS success literature into a more coherent body of knowledge that will serve as a guide for future research (DeLone & McLean, 1992). Basically, the model proposes that System Quality and Information Quality individually and in tandem affect both System Use and User Satisfaction.

Moreover, the degree and quantum of System Use can also positively or negatively affect the degree of User Satisfaction. The degree of User Satisfaction also affects System Use, whilst System Use and User Satisfaction are direct antecedents of Individual Impact. The impact on individual performance should eventually have some impact on the organizational performance. The model drew extensively from information influence theory (Mason, 1986), mathematical theory of information (Shannon & Weaver, 1949), published IS success research literature from 1981 to 1987 (DeLone & McLean, 1992; Petter et al., 2008). The original model was made of six interdependent variables: system quality, information quality, use, user satisfaction, individual impact, and organizational impact (DeLone & McLean, 1992). The model attracted various reviews and criticism resulting in several recommendations by IS researchers for modifications of the constructs and the relationships (Rai, Lang, & Welker, 2002; Seddon, Staples, Patnayakuni, & Bowtell, 1999; Seddon, 1997).

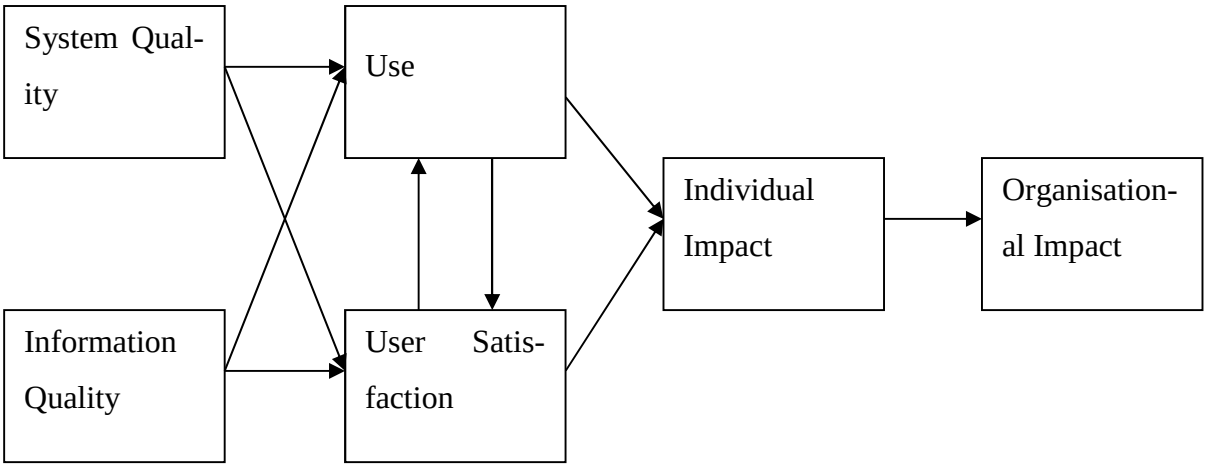


Figure 20 Delone & McLean IS Success Model (DeLone & McLean, 1992).

3.1.5 Seddon's Critique of Delone & McLean IS Success Model

Among the various critiques of the original IS success model was Seddon, (Seddon et al., 1999; Seddon, 1997). Seddon observed that, the **Use** constructs is most suitable for voluntary systems, whereas usefulness is a better measure of IS success in a situation where usage of a system is mandatory (Seddon, 1997). Hence they suggested more focus on usefulness, as in TAM (F. D. Davis, 1989). He posited that "the underlying success construct that researchers have been trying to tap is Usefulness rather than Use" as it is in the original model because of the ambiguity of the concept of use (Petter et al., 2008; Seddon, 1997). To prove that assertion, three different potential meanings of the use construct were derived. Seddon's suggestions for further modifications would however, have made the IS success model complicated, given that the D&M IS success model was intended to be complete and parsimonious.

3.1.6 The updated DeLone & McLean IS Success Model

The original DeLone & McLean IS success model has been widely applied by various IS researchers to the understanding and measurement of the IS success dimensions. The updated DeLone & McLean IS success model was presented as a response to the calls for revision and validation of the model by researchers and also offer a framework for organizing IS success measurements (Delone & McLean, 2003). After about ten years of review and constructive criticisms, DeLone and McLean evaluated the debates, challenged some of the criticisms, and introduced what they termed, an updated D&M IS success model. For instance on the issue of replacing **use** versus **usefulness,** as suggested by Seddon (Seddon et al., 1999; Seddon, 1997), DeLone and McLean, (2003) posited that "*even in mandatory systems, there can still be considerable variability of use and therefore Use as a variable must be retained"*(Delone & McLean, 2003; Petter et al., 2008).

In effect, the clarification of the use constructs in the updated model has further enhanced the model. The authors offered the following explanations with respect to "use" and "usefulness": "*Use must precede ''user satisfaction'' in a process sense, but positive experience with ''Use'' will lead to greater ''user satisfaction'' in a causal sense"* and "*increased user satisfaction will lead to a higher intention to use, which will subsequently affect Use"* (Delone & McLean, 2003; Petter et al., 2008; Sabherwal et al., 2006; Urbach & Müller, 2012). The updated model also introduces Service Quality as a new dimension following suggestions from researchers with e-commerce orientation and adopted SERVQUAL, an instrument used mostly in marketing, as an instrument for service quality measurement (Jiang, Klein, & Discenza, 2002; Petter et al., 2008; Pitt, Watson, & Kavan, 1995). Another well-known modification to the D&M model is the changes offered by (Seddon, 1997). Again the model also clarified Seddon, (1997) argument that the D&M model in its original form was confusing, because both process and variance models were combined within the same framework and hence, a shortcoming of the model. They responded with a claim that it was rather one of its strengths, since the insights provided respectively, by the process and variance models was richer (Delone & McLean, 2003). In addressing the criticism that an information system can affect levels other than individual and organizational levels since IS success affects work-groups, industries, and even societies (Myers, 1997); Seddon et al., 1999), D&M replaced the variables, individual impact and organizational impact, with net benefits, thereby accounting for benefits at multiple levels of analysis (Delone & McLean, 2003; Petter et al., 2008; Urbach & Müller, 2012). In effect the revised model now makes it possible for it to be applied in various levels of analysis that are appropriate to the researcher. The table below provides a brief description of the six dimensions of the updated IS success model:

System quality	**The desirable characteristics of an information system (F. D. Davis, 1989; Delone & McLean, 2003; Petter et al., 2008). Key measures of system quality construct include: ease of use, system flexibility, system reliability, and ease of learning, as well as system features of intuitiveness, sophistication, flexibility, and response times.**
Information quality	The desirable characteristics of the system outputs such as; management reports and credentials, etc. (Delone & McLean, 2003; Petter et al., 2008); Key measures of system quality construct include: relevance, understandability, accuracy, conciseness, completeness, currency, timeliness, and usability.
Service quality	The quality of support that the users of the system receive. For example: responsiveness, accuracy, reliability, technical competence, and empathy of the personnel staff. SERVQUAL measures the service quality of IT departments, as opposed to individual IT applications, by measuring and comparing user expectations and their perceptions of the IT department. Pitt et al. (1995) evaluated the instrument from an IS perspective and suggested that the construct of service quality be added to the D&M model (Petter et al., 2012; Pitt et al., 1995).
System use	The degree and manner at which customers utilize the capabilities of an information system (Delone & McLean, 2003; Petter et al., 2008). Some of the measures of use construct include: amount of use, frequency of use, nature of use, appropriateness of use, extent of use, and purpose of use.
User satisfaction	Users' level of satisfaction with the system's output (i.e. Reports, Web sites), and support services. Some of the measures of user satisfaction construct include: adequacy, effectiveness and efficiency (Helail Almutairi & Subramanian, 2005; Blake Ives & Olson, 1984; Seddon et al., 1999), enjoyment, system satisfaction, overall system satisfaction (H. Almutairi & Subramanian, 2005; Gable, Sedera, & Chan, 2008; Seddon et al., 1999; Urbach & Müller, 2012) the most widely used multi-attribute instrument for measuring user information satisfaction can be found in (Helail Almutairi & Subramanian, 2005; Blake Ives & Olson, 1984; Seddon et al., 1999; Urbach & Müller, 2012).
Net benefits	The extent to which IS are contributing to the success of the different stakeholders (Urbach & Müller, 2012). Some of the measures of Net Benefit include: improved decision-making, improved productivity, increased sales, cost reductions, improved profits, market efficiency, consumer welfare, creation of jobs, and economic development (Petter et al., 2008; Urbach & Müller, 2012).

Table 7 Dimensions of Updated Delone and McLean IS Success Model.

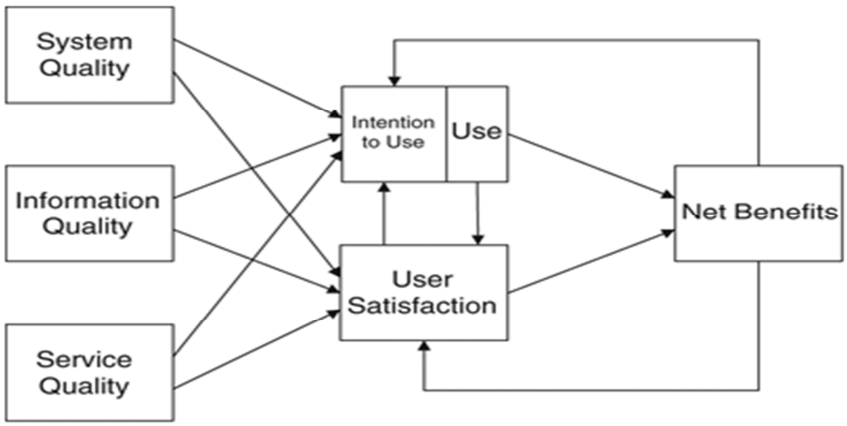


Figure 21 Updated Delone & McLean IS Success Model (Delone & McLean, 2003; Petter et al., 2008).

Petter et al. (2008) posited that the practical application of the D&M model naturally depends on organizational context. Thus researchers must have a clear understanding of the contextual details and the type of IS under study as an aid in the choice of measures. The selection of success dimensions and specific metrics also depend on the nature and purpose of the system(s) being evaluated. Petter et al (2008) observed that information system that is managed by a vendor will measure the service quality of the vendor, rather than of the IS department. Similarly there might be a commonality in the metrics used for measuring the service quality of electronic business applications whilst different measures might be used depending on the contextual circumstances. Seddon et al. (1999) developed a context matrix that is a valuable reference for the selection of success measures based on stakeholders and level of analysis. Petter et al. (2008) posited that the D&M model is applicable in a variety of contexts (Petter et al., 2008). This study adopts and adapts the updated D&M model in the context of trusted identities from a developing country perspective.

3.2. IS Success and Trusted Identity Management Systems

The conceptualization and measurement of IS success in a practical context remains complex (Gable et al., 2008). Petter et al., (2012) in their review of the past, present and the future of IS success (Petter et al., 2012) observed that defining and measuring "success" has been a challenge for the IS field, and chronicled the changes in the measures of IS success from both research and practice. In the study question, they posited that in evaluating the success of an information system, definition of the context based on the type of IS and its stakeholders are paramount (Petter et al., 2012).

The D&M IS success model has been applied in the evaluation of various private sector IS projects both at the individual and organisational level analysis. Wang & Liao (2008) have empirically validated the D&M IS success model in the context of G2C e-Government sys-

tems (Wang & Liao, 2008). Teo et al (2008) also studied the relationship between trust and e-Government (Teo et al., 2008) whereas Connolly et al (2010) recently evaluated the impact of e-government Service Quality and transparency (Bannister & Connolly, 2011a, 2011b; R. Connolly, Bannister, & Kearney, 2010). The goals of e-Government are to improve; the quality of service to citizens, efficiency of administrative processes, and to enable effective citizens' participation and engagement in the provision of government services (Grönlund & Horan, 2004; Helbig, Ramón Gil-García, & Ferro, 2009). Hence national identity management initiatives are implemented under the broad themes of e-government (G. Aichholzer & Strauß, 2009; Georg Aichholzer & Strauß, 2009). The digital age of attribute based assertions has maximised the potential for individuals to receive personalised services, customised experiences, and personalised services based on the ability to seamlessly recognise unique attributes. Thus, two different individuals, using the same keywords in Google, would receive different outcomes for their search results. Unfortunately, empirical studies and theories on the application of IS success model for national digital identity management projects are almost indiscernible. Yet governments implement digital identity policies with the aim of improving citizens' interactions, policy coordination, national security, etc. This complicates efficient measurement of system's effectiveness since systems must create value for all stakeholders concurrently, making effectiveness a relative concept. It is therefore imperative that scholarly encouragement to focus on developing models for evaluating and effective privacy enhancing trusted identity management systems. This will help in extending our understanding of the essential requirements for information system success which also address the issues of trust and privacy.

3.2.2 Stakeholder Analysis

Freeman, (1994) defined stakeholders as "any group or individuals who can be or are affected by, the achievement of an organizational goal" (Crane & Ruebottom, 2012; Freeman, Harrison, & Wicks, 2007; Freeman, 1994). Broadly, stakeholders could be subdivided into two:

- The primary stakeholders – those with formal or official contractual relationships with the company, such as clients, suppliers, employees, shareholders, among others;
- The secondary stakeholders – those without such contracts, such as government authorities or the local community.

Stakeholder theory has been discussed from three main perspectives – descriptive, normative, and instrumental approaches (Crane & Ruebottom, 2012; Donaldson & Preston, 1995; Jones & Wicks, 1999). The descriptive stakeholder theory focuses on the characteristics and behav-

iour of stakeholders and how an organization interacts with them (Crane & Ruebottom, 2012). This viewpoint has been criticized for its lack of clear objectives (Treviño & Weaver, 1999).

The normative perspective on the other hand is rooted in business ethics and corporate social responsibility literature (Clarkson & others, 1998; Freeman et al., 2007), and focuses on principles of fairness and of common good that organisations must observe, (Harrison, Bosse, & Phillips, 2009; Phillips, Freeman, & Wicks, 2003). The normative stakeholder theory has also received many criticisms from pro-business researchers on the basis that the responsibility of businesses is to increase its profits and that "the business of business is business and that businesses do not set social policy but rather look up to the government for social policy (Clarkson & others, 1998; Friedman & Miles, 2002, 2006).

Lastly, proponents of the instrumental stakeholder theory assert that policies that are based on a comprehensive analysis of stakeholder priorities lead to broader consensus (Scott, Golden, & Hughes, 2004). Instrumental stakeholder analysts focus on organizational consequences considering the interest stakeholders in management decision making by examining the connections between the practice of stakeholder management and the attainment of various corporate governance goals (Clarkson & others, 1998). According to (Flak & Rose, 2005, p. 657) *"clear understanding of stakeholders in e-government, combined with an understanding of e-government's potential effects, enables policymakers to develop e-government in ways that are likely to benefit the majority of stakeholders."* Digital identity policies are types of electronic governance, and for that matter, it is very important to involve all the interest groups to achieve the desired goals. Stakeholder theory is also beginning to gain acceptance in e-government research (Chan & Pan, 2008; Esteves & Joseph, 2008). Democratic societies enjoin leaders to carry out the will of the people. For that matter, stakeholders with divergent views must be considered in e-government initiatives. Zhang et al. (2005) in their descriptive stakeholder study identified four subgroups of stakeholders in an e-government initiative: Government agencies, local governments, nonprofit organizations, and private companies and suggested the need to reconcile their divergent/convergent opinions on the implementation of e-government initiatives. (A. O. Laplume, Sonpar, & Litz, 2008) detected a paucity of studies on stakeholder perspectives in addition to the methodological gaps worth addressing. For instance, it was observed that qualitative methods have been underused, even though these methods offer an advantage for their "ability to seek clarifications and confirmation of evidence by cross-validating data. Qualitative research is interesting and can provide memorable examples of important management issues and concepts that enrich the field" (A. Laplume, Sonpar, & Litz, 2008, p. 1175).

Stakeholder Approach	Theoretical Underpinnings	Main Criticism
Descriptive: **Understanding the relationship between an organization and its stakeholders**	Organisational behaviour	Unfocused: aims of descriptive stakeholder theory are unclear, what is it trying to prove or disprove?
Normative: **organizations should take all stakeholders into consideration, as a moral responsibility**	Corporate social responsibility; Common good theory	"Business of business is business" businesses are not charities, but profit making entities.
Instrumental: **Organizations should take key stakeholders into consideration as this leads to success and competitive advantage.**	Business and management	Stakeholder involvement is not feasible and/or is not always linked to organizational success.

Table 8 Summary of stakeholder theory.

3.2.3 Adapted DeLone & McLean IS Success Model

Petter et al., (2012) observed that the undue focus on the classic IS tripartite model, where there are only three primary actors or stakeholders (developers, users, and managers) tend to diminish the value of IS success literature to research with macro perspective. They therefore posited that *"to be valuable, IS success measures must capture all of the stakeholders, and yet be reasonably parsimonious in order to be useful to the researcher and to the practitioner"(Petter et al., 2012).*

The updated D&M IS success model is therefore adapted in this study from a societal perspective. This type of study is new to both IS success and identity management literature given that none of the recent IS success research have focused on IdMS as shown in Table 10. The study highlights the important role of trust and information privacy, described in Chapter 2, in effective IdMS. Many user-centric and trusted IdMS models and initiatives have been proposed (Grant, 2011a; 2010; Microsoft, 2011).

A key requirement of a trusted and citizen-centric identity management systems is to ensure the cooperation of all stakeholders within the identity ecosystem (Grant, 2011a). We propose a conceptual model for a trusted identity framework based on the Delone and McLean IS success model. Since national identity transcends individual and organisational level of analysis to become a societal issue, we adapted the model by examining the definition of the dimensions and excluded those that are not applicable to a trusted identity framework within a societal context. The adapted constructs are explained in Table 7.

System quality	Citizens do not only consider performance characteristics, functionality, and ease of use of the system but also the skill set of the people, availability of documentation and the reliability of the processes. This is in line with the definition of information systems, which is the combination of technology, people, procedures and processes (O'Brien & Marakas, 2010). For instance, if the system has all the attributes as described in success (Delone & McLean, 2003; DeLone & McLean, 1992; Petter et al., 2008, 2012; Urbach & Müller, 2012) with no skilled personnel to run it or ineffective processes, the performance of the system can be affected as well as the trustee's relationship with the trustor.
Information quality	Information quality is the degree to which the information produced by IdMS is accurate, relevant, complete and in the right format (Schaupp, Fan, & Belanger, 2006). Information is said to be of good quality when it is useful, timely, cost effective, reliable and understandable. These are critical factors in identity management systems, and plays a prominent role in affecting how all the stakeholders in the identities ecosystem trust the system and each other (Petter et al., 2008; Schaupp et al., 2006).
Service quality	Service quality is used to measure the overall support that users receive from service providers. Key aspects of service quality; responsiveness, reliability, empathy, competence (Delone & McLean, 2003; DeLone & McLean, 1992; Petter et al., 2008, 2012; Urbach & Müller, 2012).
User empowerment	User empowerment is the extent of user participation in decision making, the users' ability to exercise a degree of control over their personal information or their informational self-determination, and to have confidence that third parties respect their privacy (Biskup & Brüggeman, 1988). Previous research found that individuals who believe they can exert more control over events, such as the secondary use of personal information, are less likely to perceive that their privacy is being invaded (Tolchinsky et al., 1981). When users are involved and empowered they are more likely to have positive attitudes toward secondary information use and hence will also have a lower concern for privacy. Deci et al (1989) have posited that self-determined individuals experience a sense of freedom to do what is interesting, personally important, and vitalizing (Deci, Connell, & Ryan, 1989a). User empowerment therefore leads to state of belief in individuals that they can influence the system of which they are an integral part.
Institutional cooperation	This describes the aspects of key stakeholders working together to ensure interoperable laws, technologies, systems and standards. This type of collaboration also leads to effective communication and compliance with standards with the identities ecosystem.

Use, user satisfaction	In many countries the use of government provided credentials are mandatory due to the coercive power of government and for that matter user satisfaction will be the best measure of the success. The trusted identities framework describes how stakeholders in the identity ecosystem trust each other and not necessarily the use of the credentials or services by the service provider's systems. Hence the use and user satisfaction dimensions are merged as one construct since it is the satisfaction that give the user confidence for repeat purchases. (Delone & McLean, 2003; DeLone & McLean, 1992; Petter et al., 2008, 2012; Urbach & Müller, 2012). User satisfaction is achievable in a situation where stakeholders trust each other and privacy concern is low. The relationship between privacy concern and trust is illustrated in Figure 23.
Net benefits	Net Benefit describes the extent to which IS promotes the interest of the different stakeholders (Urbach & Müller, 2012). In a trusted identities environment, the ultimate success will be where the threshold point of privacy concern trust is met. Net Benefit in this regards is measured by the level of institutional cooperation, technology, policy regulatory framework interoperability, opportunities for secondary uses of personal information, attribute based credential technologies etc.

Table 9 Dimensions of Adapted DeLone & McLean IS Success Model.

Where there is a positive perception of trust and privacy among the stakeholders in an identity ecosystem, and the services they provide, it can engender collaborative environment and more innovative use of personal information for secondary purposes.

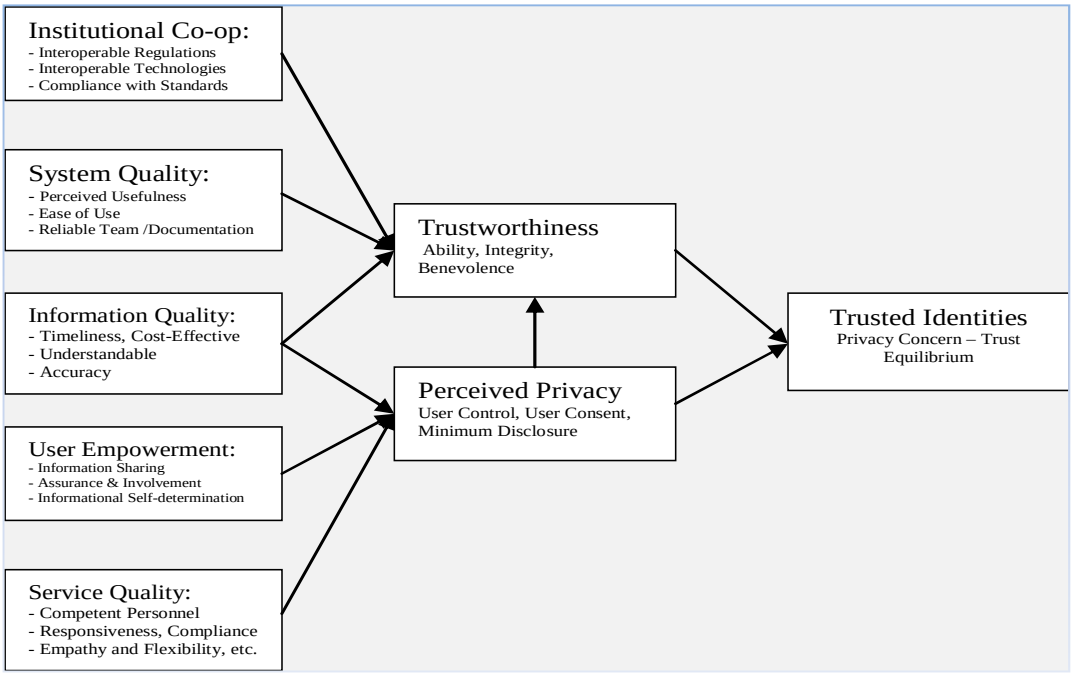


Figure 22 Trusted Identities Framework.

Figure 22 describes the trusted identities framework. Institutional cooperation has a positive influence on trustworthiness. Interoperable laws, technologies, policies and standard are typical examples of institutional cooperation. Also, strict enforcement of regulation and the ability to seek redress are also signs of institutional cooperation. Systems' quality and information quality have also a positive relationship with trustworthiness. Usefulness and ease of use (F. D. Davis, 1989; Delone & McLean, 2003) skilled and reliable credential issuers signify their abilities whilst information signifies integrity on the part of the identity and relying parties. These are the attributes of trustworthiness (Roger C. Mayer, Davis, & Schoorman, 1995a). User empowerment, information quality and service quality have the potential of minimizing societal privacy concerns. Positive societal privacy concerns are signs that identity and service providers are benevolent – which is an attribute of trustworthiness. Trustworthiness and positive privacy concerns result in a trusted identities ecosystem.

Research Focus	**Authors**
Data warehouse	Nelson et al. (2005), Wixom and Todd (2005)
e-Commerce system	Wang (2008)
Enterprise system	Lin et al. (2006), Qian and Bock (2005), Sedera (2006)
Finance and accounting system	Iivari (2005)
Health information system	Yusof et al. (2006)
Intranet	Hussein et al. (2008), Masrek et al. (2007), Trkman and Trkman (2009)
Knowledge management system	Clay et al. (2005), Halawi et al. (2007), Jennex and Olfman (2003), Kulkarni et al. (2007), Velasquez et al. (2009), Wu and Wang (2006)
Learning system	Lin (2007), (2012) , (Alsabawy, Cater-Steel, & Soar, 2012; Lin & Wang, 2012)
Online communities	Lin and Lee (2006)
Picture archiving and communications system	Pare et al. (2005) Portal Urbach et al. (2009a), Urbach et al. (2010), Yang et al. (2005)
Web-based system	Garrity et al. (2005)
Web sites	Schaupp et al. (2006)
Payment Systems	(Sørebø & Fuglseth, 2012)
Underground Pipeline Systems	(Cheng, 2012)

Table 10 Recent Applications of IS Success Model.

3.2.4 Privacy Concern-Trust Curve

Generally, societal interactions and business relationships begin from a low level of trust (distrust) and high privacy concern. With the disclosure of more information, strong institutional cooperation, stakeholder involvement and awareness exposure to the technology, they begin to exercise some degree of user control over their personal information. Such informational self-determination results in the establishment of a certain level of trust. Thus, citizens become more empowered and revise their negative perceptions about the IdMS and identity service providers. This establishment of trust reduces the initial privacy concerns. In principle, a low level of trust is associated with a high privacy concern, whereas a high level of trust is associated with low or reduction in privacy concerns. Thus, the mediating and moderating effect of trust can result in either a negative or positive societal attitude change towards IdMS.

The qualitative relationship between trust and privacy concern is shown in Figure 23. A certain threshold level of trust must be overcome, before the citizens are ready to open up for interaction. The figure also shows that absolute trust or zero privacy concern is not possible within a trusted identities environment, and hence the curve can only asymptotically approach the two axes. The purpose of the trust framework therefore is for society to establish the framework that can overcome the trust threshold. Beyond this level, trust and privacy is adequate to encourage more collaboration, creation of new identity-based services, institutional collaboration, etc.

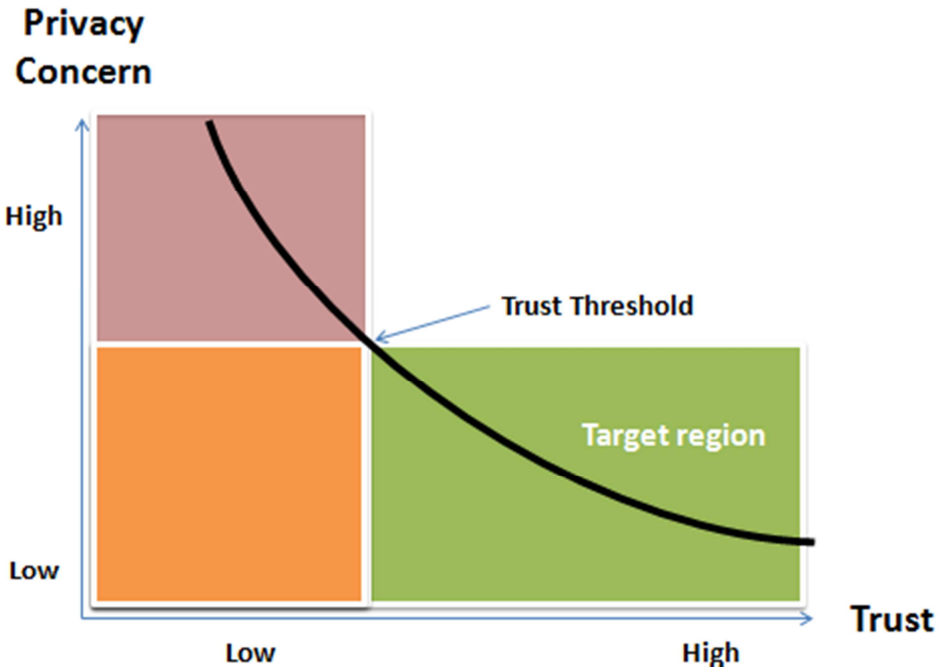


Figure 23 Privacy-Concern-Trust Curve.

3.3 Summary of Theoretical Perspectives

This chapter has demonstrated how relevant literature drawn from different domain was integrated in constructing a framework for evaluating citizen-centric trusted identities environment. This study has carefully addressed the caveat that researchers should not merely apply existing theories in a new context as this may potentially hinder the discovery of aspects unique to the artifact under study (Sarker & Wells, 2003). The updated DeLone and McLean IS Success model form the core of the discussion but it is expanded and modified based on the findings from Ives, (1984) user involvement theory, stakeholder theory, trust and information privacy. This approach to research has given a strong methodological support and opportunity for scholarly manifest and acceptance (V. Venkatesh & Davis, 2000) among IS success researchers. As it has been suggested by earlier scholars, the relevancy and applicability of approaches can be developed by adopting ideas and constructs from research which are either consumption, process or socially oriented so long as there is a clear understanding of the motivations and contextual issues (P. E. Pedersen, 2003). This is the approach adopted in this study.

Chapter 4 Research Methodology, Approach and Design

4.1 Introduction

The absence of evidence is not evidence of absence ……. There are no "knowns". There are things we know that we know. We also know there are known unknowns; that is to say, we know there are some things we now know we do not know. But there are also unknown unknowns – the ones we don't know we don't know.

So when we do the best we can and we pull all this information together, and we then say well that's basically what we see as the situation, that is really only the known knowns and the known unknowns. And each year, we discover a few more of those unknown unknowns[22].

Donald H. Rumsfeld

Confused as they may seem, the above quotation reflects the importance of scientific inquiry and the need for systematic due diligence and multiple probes in all scientific inquisitions, although the obvious is simply missing in the quotation; "*the knowledge we do not want to know*" (Daase & Kessler, 2007). These are things we could know but rather decide not to know by either discounting it as irrelevant or simply repressing their relevance. Hence it is the appreciation of what we do not know, what we cannot know and what we do not like to know; and our ability to address the relevance paradox that determines our cognitive frame.

The world-view, knowledge and assumptions that researchers bring to bear on a particular study can immensely impact on the research paradigm[23], ontological and epistemological assumptions, conclusions drawn and lessons learnt, and also contributes to the evaluation of theory construction (Walsham, 1995, 2006). I present the research philosophy, methodology, the research design and methods in this chapter. Such reviews are greatly influenced by the philosophical paradigm underpinning the study and my ontological and epistemological views. I also present the limitations of my relation to the research design and the approach including the methodological contributions identified in this study.

---

[22] US Defense Secretary, Press Conference at NATO Headquarters, Brussels, Belgium, June 06, 2002. http://www.defense.gov/transcripts/transcript.aspx?transcriptid=3490

[23] A paradigm is a worldview, or a way of thinking that reflects fundamental beliefs and assumptions about the nature of phenomena. An ontology, ultimately, is how one sees and views the world and reality. It is an agreed upon theory, world view, or methodology embodied in the beliefs, practices and products of a group of scientists (A. Tashakkori & Teddlie, 2010, p. 85)

This chapter is a logical progression of the phenomena[24], research objective and rationale of the study as presented in Chapter 1, the state-of-the-art and context in Chapter 2 and then the theoretical framework in Chapter 3.

4.2 Research Philosophy

Philosophy, *'the love of wisdom* (Cavalier, 2003; Gregory, 2012) tends to be viewed as the business of philosophers (Ruona & Lynham, 2004), although it has a very practical purpose and intent, coupled with its utility to inspire learning. Rouna & Lynham, (2004) observed that; *"how we think about the world shapes and directs how we act in the world; and how we act in the world, in turn, reflects and influences how we think about and consequently see the world"*. Therefore the declaration of one's philosophical stance is vital to the critical evaluation of the research, since many researchers can arrive at different conclusions given their varied world view, in dealing with similar research phenomena, questions or hypothesis (Pring, 2000). Thus researchers must clearly explicate the philosophical assumptions and their axiological, ontological, epistemological and methodological concepts.

Generally, philosophical discourse is concerned with the issues of; being (ontology), knowing (epistemology) and acting (axiology) (Denzin & Lincoln, 2000, 2011; Fielding, 1999; Ruona & Lynham, 2004). To explicate the trajectory between these philosophical stances, I deem it necessary to elaborate on the philosophical stances.

Ontology focuses on the assumptions about the nature of phenomena, thus the nature of reality and nature of human beings as they are in the real world (Gioia and Pitre 1990). It focuses on basic questions and assumptions about what is reality? As in Rouna & Lynham, (2004), the following are some ontological question; *What is 'there' and what do we mean by 'there'?, what is the world made of?, Is reality ordered in any way?, is reality 'out there' or 'inside us' or a combination of both?, what are humans?* (Ruona & Lynham, 2004).

Epistemology Epistemology (also described as the theory of knowledge) is the component of philosophy that raises questions about the nature of knowledge and reasonable belief (Bryman, 2012). It focuses on the nature of and scope of knowledge, and the relationship between the inquirer, the knower and/or the known (Denzin & Lincoln, 2011). Thus, epistemology makes fundamental assumptions about the nature of knowledge about a phenomena (Denzin & Lincoln, 2011; Gioia & Pitre, 1990, p. 585; Ruona & Lynham, 2004). In so doing, it ad-

[24] Any incident deserving of inquiry and investigation, any event that is observable or any observable occurrence

dresses questions like: w*hat is knowledge?, how does knowledge differ from mere opinion or belief?, How is knowledge acquired?* In other words should the social world be studied like in natural sciences, following the same principles, procedures and ethics or otherwise? Hence epistemological inquiry is about how the subjective and objective relationship between the researcher, the phenomena of interest and what he seeks to know about it. In essence, epistemology is about how we know and think about the world.

Axiology play a vital role in adhering to the standards and requirements of acceptable methodology and methods in research and practice (Ruona & Lynham, 2004; Abbas Tashakkori & Teddlie, 2010). Axiology is also described as ethics in scientific inquiry and focuses on what is good, what ought to be done, how a researcher should act, and the extent to which researchers' actions are in congruence with the ontological and epistemological ideals (Ruona & Lynham, 2004; Abbas Tashakkori & Teddlie, 2010; Teddlie & Tashakkori, 2012).

Methodology – Philosophical questions and assumptions are usually elucidated in the light of the systematic organization of the research, the methods employed, and in the manner in which the findings and conclusions are presented. Methodology is the means by which comprehension of a research phenomena is generated (Denzin & Lincoln, 2011; Abbas Tashakkori & Teddlie, 2010). Thus methodological questions deal with how the inquirer can set forth to find out what they believe exist and can be known or otherwise (Denzin & Lincoln, 2011; Abbas Tashakkori & Teddlie, 2010).

4.2.1 Philosophical Paradigm

Kuhn's (1996) observed in his *structure of scientific revolution* (Bird, 2012; Kuhn, 1996) that the paradigmatic manifestation of the work of a researcher is a reflection of the sets of his/her congruent assumptions and worldview. Thus, Guba and Lincoln (1994), and in their recent study, Guba et al., (2011), identified five underlying paradigms for research: positivism, post-positivism, constructivism/interpretivism, critical and participatory (Lincoln et al., 2011, 2011). The findings from the work of Orlikowski and Baroudi's (1991) showed a majority of IS publications had a positivist anchoring followed by interpretivism. This study discusses only the first three since they are relevant either in their application or for comparison. Post-positivism and constructivism are considered relevant for my study as it is also consistent with Chen & Hirschheim, (2004) paradigmatic bracketing of IS research (Chen & Hirschheim, 2004).

4.2.2 Positivism

Positivism is an epistemological position that argues for the application of natural science research methods to the study of social reality (Bryman, 2012). In his book, social research methods, Bryman catalogued the positivism principles as: "*the purpose of theory is to generate hypotheses that can be tested in order to explain laws (deductivism principles); Knowledge is the outcome of gathering of facts that provides the basis of laws (inductive principle); Science must be conducted in an objective manner; and that scientific statements are the true domain of scientists and must be distinguished from normative statements".* Similarly, Lee, (1991), describes positivism as "*the manipulation of theoretical propositions using the rules of formal and hypothetico-deductive logic, so that the theoretical propositions satisfy the four requirements of falsifiability, logical consistency, relative explanatory power, and survival"*(A. S. Lee, 1991). Thus Positivist studies an objective world, measures physical and social phenomena in order to characterise them and predict their behaviour. In an attempt to increase predictive understanding of phenomena, positivist studies usually serve primarily to test theory. In essence positivist researchers tend to believe in achieving a 'scientific' ideal by objectively being detached from the phenomena under investigation. This is in contrast with post-positivist research as it is grounded on the centrality of meaning (and often language) to human affairs (Sharp et al., 2011).

4.2.3 Post-Positivism

Post-positivism, seen as a mild form of positivism, is often described as the "natural-science model" of social science (A. S. Lee, 1991). While positivists believe that the researcher and the researched person are independent of each other, postpositivists accept that theories, background, knowledge and values of the researcher can influence what is observed.[1] However, like positivists, postpositivists pursue objectivity by recognizing the possible effects of biases. Post-positivists believes that the social world is sought and explained under assumptions and with procedures and evaluation criteria similar to those of the natural sciences. Thus, post-positivists focus on examining how phenomena are understood by relevant actors, and how these different understandings and values play out in research. Ontologically, post-positivists are pitched against critical realism, and belief in a 'real' reality – a reality 'out there'. Moreover post-positivists maintain the epistemology of objective and detached stance both in relation to the phenomenon being investigated and to the knowledge which can be derived from it. Hence post-positivist conducts rational analysis of data in a mental problem space by constructing deductive arguments of cause-and-effect" (Boland & Day, 1989, p. 353). The methodological principles applied by post-positivists for obtaining knowledge about phenomena focus on the verification or falsification of the hypothesis using statistical

inferences, structural equation modeling, mathematical analysis and experimental and quasi-experimental test designs (A. S. Lee, 1991; Lincoln et al., 2011).

4.2.4 Interpretivism (Constructivism)

Interpretivism is an alternative or the contrasting epistemology of positivism (Bryman, 2012; Chen & Hirschheim, 2004; Lincoln et al., 2011; Teddlie & Tashakkori, 2012). Interpretivism is predicated on the premise that the differences between people and natural science objects must be respected and thus there is the need to grasp the subjective meaning of social action (Bryman, 2012). Interpretivists world view therefore of phenomena – people and institutions, is different from that of positivists. Intrepretivists see the distinctiveness of human behaviour and try to understand such behaviour as opposed to explaining human behaviour based on natural logic which is in the realm of positivism. According to Henning et al (2004), the interpretive paradigm places emphasis on experience and interpretation which is concerned with meaning. Thus, it seeks to unearth the way a given society understand a particular phenomena. Intrepretive inquires, in essence, are about producing descriptive analysis with the intention of highlighting deep understanding of the phenomena.

Hence the ontological world view of interpretivism is that social phenomena and their meanings are continually being constructed (Constructivism) by social actors and thus is in a constant state of revision (Bryman, 2012). Thus ontologically, reality is seen as actively, locally and socially constructed and specific to actors or groups of actors (Lincoln et al., 2011). This state of constant revision implies that researchers only present specific version of social reality and definitive reality which is their construction of the social reality. Hence in constructivism, there is a thin line between ontology and epistemology given that knowledge is seen as very subjective and indeterminate (Bryman, 2012; Grene, 1967). In effect knowledge acquisition straddle between subjective and intersubjective characters resulting from the interaction between the inquirer and the knower/agent. Phenomenology, interpretive case studies and ethnography methodologies conform to interpretivism/constructivism paradigm.

4.3 Methodological Considerations & Justification

This study adopts interpretive ontology and epistemology in forming my understanding of citizen centric trusted identity management phenomena. Such a stance is what influenced my empirical data collection, since interpretation of the world and reality construction is a common occurrence in many spheres of human endeavour (Shils & Finch, 1949).

4.3.1 Methodological Considerations

Klein & Myers, (1999) have described IS research as interpretive on the assumption that"our knowledge of reality is gained only through social construction such as language, social consciousness, shared meanings, documents and artifacts". Given that the study of information systems entails both computer science and its application in various shades of management and society, by implication, information systems research falls within social science research. Hence it focuses on the understanding that is based on reality since information system is not only concerned with technological systems design and development but also it is concerned with core aspects of planning, management, implementation, evaluation and maintenance. According to Schutz, (1954) and recently in (Bulmer, 2011; Weber, Shils, Finch, & Antonio, 2011) the primary goal of social science is to obtain organised knowledge of social reality – "what the actor "means" in his action, in contrast to the meaning which this action has for the actor's partner or a neutral observer" (Schutz, 1954).

Axiological considerations: My axiological position is that ethos and values can influence the learning process and what should be legitimately reported. Thus in questioning it is important to respect the privacy of respondents such that what is reported does not expose certain vital respondents information or lead to privacy intrusion.

Ontological Considerations: National identity management systems are not seen as a single identity management system by a particular institution but the entire identity management policies of a nation. Hence there are various stakeholders in the identity ecosystem comprising; policy makers, credential issuers, relying parties, standard agencies, citizens and businesses whose core activities are offering services to either credential issuers or the relying parties. The idea of citizen centric trusted identities is that individuals have the liberty to present claims that can be verified and also depending on the context certain information will be revealed. However the requirement for user control with respect to the identity presuppose a literate society, exposed to modern technology.

Additionally, civil registration systems are usually the prime source for issuing trusted credentials but in many developing countries, civil registration systems are not reliable, giving room to various forms of identity abuses. The reality is that in a developing country like Ghana, there is a high rate of illiteracy and lack of exposure to modern technology. Also due to a lack of universal means of identification, there is the tendency of using certain credentials issued for a particular purpose (e.g. Driver's license, voter ID card) as proof of identity. Internet connectivity remains a challenge, due to comparatively high cost to citizens and lack of

adequate infrastructure that hinder access to many which in the end hinders online identity verification and identity service provision.

In effect, the reality (ontology) is that trusted identities require the cooperation of the key stakeholders and policy makers who understand and are capable of addressing the contextual issues in order to achieve success. This means that technology is not the panacea in national identity policy but must only act as a medium for addressing the contextual identity management issues.

Epistemological considerations. Given that the reality of the context affects the mode of learning and the knowledge acquired, it is thus implied that the acquired knowledge will not conclusively pass objectivity test. It is therefore important to emphasize that objectivity is a positivist epistemological stance. Interpretive studies are usually subjective and inter-subjective, as it is in the case of this study in the sense that selection of key stakeholders involves some level of subjectivity. I maintain a middle position between the foundationalist and the critical epistemologies since it offers me access to the local realities constructed by people that interact with the credentials in their day to day transactions and interactions. Such a world view is thus of a subjective (Lincoln et al., 2011) character where findings are constructed and reconstructed interpretively based upon theory and the data the inquirer gathered from credential issuers and citizens. From this position, it is acknowledged that more or less context specific ideas and meanings can exist within a peculiar circumstance. I do not aim to present a pure and unencumbered first person/first-level subjective understanding (Verstehen[25]) (Boland & Day, 1989; A. S. Lee, 1991). I rather participate in the discussion with the aim of focusing the discussion towards addressing perceived understanding (Denzin & Lincoln, 2000; Lincoln et al., 2011).

Cultural orientation and human cognition can be very subjective, and has the tendency of giving meaning to perceptions and interpretation of human actions within a particular context. Such human behaviours reveal inter-subjectivity of human understanding which is pertinent in this study. In this study, I strive to understand the underlining factors that influence citizens' centered, trusted identity management systems and also how identity information can be

[25] Verstehen describes the process of understanding the underlying meanings of individual and social behaviour. Thus it differentiates the social world from the natural world (Lee, 1991).

used for legitimate secondary purposes, and in essence it is important to examine their interpretive meanings and social reality. This is more so since it offers me the opportunity to have a clear understanding of the context and the counter influences of the stakeholders on identity management systems and vice versa (Walsham, 1995, 2006). This world view does not run in consonance with positivist and post-positivist research approaches in that we do not prove or disprove hypothesis within a controlled environment (Bryman, 2012; Lincoln et al., 2011).

Thus, the choice of interpretivist approach and also taking cognizance of Klein & Myers, (1999) set of principles for conducting and evaluating interpretive field studies in IS (Klein & Myers, 1999). The ontological and epistemological foundations of the interpretivist world view provided the basis of understanding of the key issues for theory development in this study. In conducting this study, I was careful not to base my analysis of IdMS and IS success solely on the existing formulations and conceptualizations. Rather, evidence were understood and analysed within their context of emergence, taken into consideration, the shared views, experiences and perceptions of the subjects, and guided by the philosophical assumptions of IS Success Model.

4.3.2 Methodological Justification

This study adopts an interpretivist stance, with the subsequent reasons accounting for the choice of paradigm. In the first place, to understand the factors that lead to a trusted identities ecosystem in a nation, it was important that I interact with the key stakeholders to understand the issues from their perspectives and for the stakeholders to discuss their individual differences. It is however not possible and also undesirable that I can unravel all intimate detail through the interactions since adherence to ethics require that the subjects require space and certain questions needed to be avoided.

Secondly, in order to be sensitive to the contextual factors and the resulting impact of associated changes, delimiting the phenomena of interest from the context (as it is in the case of positivist research) would have been incorrect given that citizen centric trusted identities are societal issues rather than a specific organisation. Thus, the phenomena cut across various segments of society. This requires an experiential knowledge which is different from what is acquired in a controlled environment. It is this background that has shaped my axiological, ontological, epistemological and methodological positions. It is however worth noting that, how I approached the study of the phenomena of interest, the related research questions were the direct results of the research design.

Thirdly, due to the dearth of literature on the measures of IdMS effectiveness from developing country perspective, this study began with an initial exploration of Identity management subject matter and the contextual issues.

Moreover secondary research on identity management concentrates on technical and technological specifications and hence existing theories have not been tested or applied within the context of national electronic identity management. Although the concept of identity is not new, the digital representation of a real person is still a new research area and hence, I believe the reality is constantly changing with the unfolding interactions and deeper interpretive insights emerging over time.

	Positivist Paradigm	**Interpretivist Paradigm**
Basic beliefs and world view	The world is external and objective	The world is socially constructed and subjective
	Observer is independent	Observer is part of what observed
	Science is value-free	Science is driven by human interests
Research Design	Quantitative	Qualitative
Research Approach	Deductive	Inductive
The researcher should	Focus on facts	Focus on meanings
	Look for causality and fundamental laws	Try to understand what is happening
	Reduce phenomenon to simplest elements	Look at the totality of each situation
	Formulate hypotheses and then test them	Develop ideas through induction from data
Preferred methods include	Operationalising concepts so that they can be measured	Using multiple methods to establish different views of phenomena
	Taking large samples	Small samples investigated in depth or over time

Table 11 Summary of Interpretive Versus Positivist paradigms.

4.4 Qualitative Research Design

> The real purpose of scientific methodology is to ensure that nature hasn't led you to believe that you know something you don't really know. Robert M. Pirsig[26]

[26] Quotation from "Zen & the Art of Motorcycle Maintenance An Inquiry into Values" by Robert M. Pirsig

Quantitative research is concerned with the collection and analysis of data in numeric form by assigning numbers to perceived qualities or variables in the description of a phenomena (Henning, Van Rensburg, & Smit, 2004). Stauss and Corbin (1998) on the otherhand has described Qualitative research as a type of research that produces findings not arrived at by statistical procedures or other means of quantification.

Based on my interpretive research world view, as explained previously, there was the need to adopt a research design that offers the opportunity to unravel all the tenets of reality and the comprehensive knowledge acquisition using various data collection methods. A Qualitative research approach is adopted in this study. Myers (1997), in drawing a distinction between qualitative and quantitative research described qualitative research as "a subjective approach which includes examining and reflecting on perceptions in order to gain understanding of social and human activity" (Myers, 1997). Qualitative research strategy is used in social sciences to enable the researcher to inquire about socio-cultural phenomena often within a given context. Case study, ethnography and action research are some of the common qualitative research strategies. In qualitative research, the major sources of evidence include observation, interviews, questionnaires, documents and texts, including the researcher's impressions of the phenomena and the context (Myers, 1997). Quasi statistics (Becker, 1970; Maxwell, 2010) were also used in a survey to identify citizens' concerns on national identification systems and also to specify contextual issues. Quasi Statistics generally, refer to the use of simple numerical results that can be readily derived from the data. Quasi-statistics allow the researcher to support inherently quantitative claims, and enable easy assessment of the amount of evidence in data bearing on a particular conclusion. – i.e. how many different sources they were obtained (Becker, 1970; Maxwell, 2010).

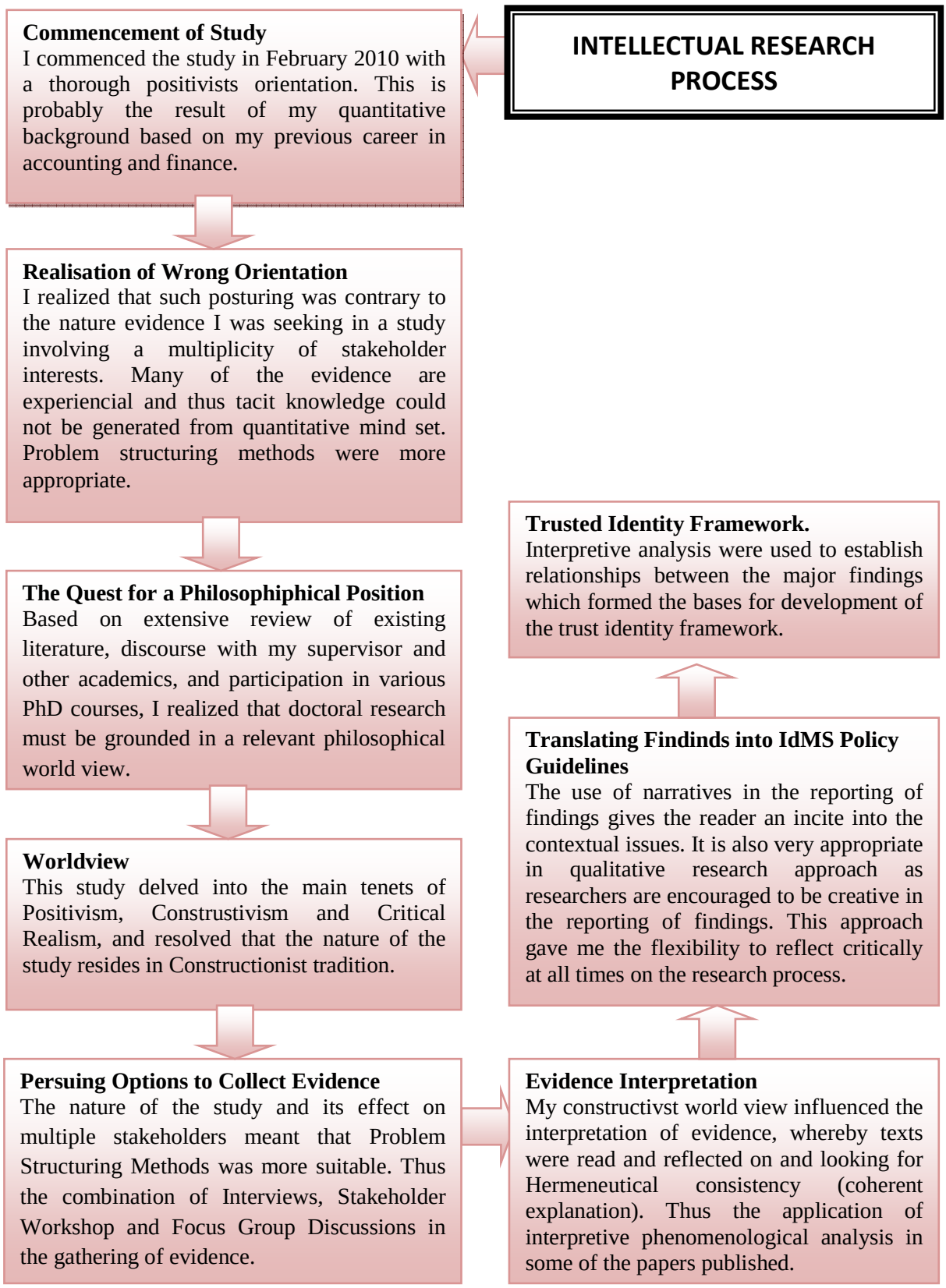


Figure 24 Intellectual Research Process.

4.4.1 Case Study

According to (John W Creswell, 2007a) a case study research involves the study of a phenomena explored through one or more cases within a setting/context (cases) or multiple set-

tings (cases). It also involves a detailed in depth data collection from multiple sources of data (e.g. Observations, interviews, audiovisual material, and documents and reports) (Creswell, 2007b). A case study was deemed most appropriate because, it is considered a very good strategy in finding answers to how and why questions, which is within the remit of my inquiry. Again, a case study is most appropriate in situations such as where the inquirer does not have control or cannot exercise significant influence on the behavioural outcomes of contemporary events (Yin, 2008a).

Hence the inquirer is faced with reality, a major requirement in the interpretivist paradigm. Gillham (2000) also advocates triangulation as a method of validating the research, as does Yin (1994:91), stating that, "a major strength of the case study data collection is the opportunity to use many different sources of evidence." T*riangulation,* often derived from navigation, pertains to the goal of seeking three or more ways of verifying or corroborating a particular event, description, or fact being reported by a study with the aim of strengthening the validity of a study (Yin, 2011a). Each of the data collection methods used in this research project could be considered part of an overall approach to improving the quality and validity of the research data through an approach known as triangulation.

Darke *et al.* (1998), for example, advocated the use of triangulation to avoid bias on the part of the researcher, either in terms of the influence the researcher has on the behaviour of participants or in terms of the bias the researcher brings himself into the conduct of the research. Triangulation is an approach intended to increase the quality and validity of the qualitative research methods and in minimising the potential sources of bias (Darke *et al.,* 1998; Myers, 1997; Patton, 2002; Stake, 1995; Yin, 1994). Stake (1995:114) said that triangulation includes, "data triangulation (from other sources), investigator triangulation (use of observers), methodological triangulation (using multiple sample types and sources)." The strategy has been categorized into three phases as follows:

1. Phase 1 – Explore Identification systems in Ghana and comparing the systems with the existing situation in OECD countries.
2. Phase 2 – Explore the causes of identification challenges in developing countries with Ghana as a case study.
3. Phase 3 – Explains the reasons for the challenges and propose guidelines for trusted identities policy formulation

SOURCES OF LEARNING	TIME LINE							RESEARCH PHASES
	Feb 2010 Jul 2010	Aug 2010 Jan 2011	Feb 2011 Jul 2011	Aug 2011 Jan 2012	Feb 2012 Jul 2012	Aug 2012 Oct 2012	Nov 2012 Jan 2013	
PhD Courses	RELEVANT PHD COURSES							ALL PHASES
Conceptual Study	LITERATURE REVIEW							
Publications and Reviews			PAPER WRITING, PARTICIPATION CONFERENCE AND REVIEW OF PAPERS					
Fieldwork 1		SURVEY	INTERVIEWS					PHASE 1
Fieldwork 2				WORKSHOP				PHASE 2
Fieldwork 3					INTERVIEWS	WORKSHOP & FOCUS GROUP		
Integration						DISCUSSION OF FINDINGS		PHASE 3
Final Thesis Preparation							THESIS PREPARATION	
RESULTS	1st Study Plan	Final Study Plan	Paper 1 & 2	Paper 3	30 ECTS	Papers 4, 5 & 6	Final Thesis Submission	**END**

Figure 25 Research Design.

Phase 1: I approached this phase of the study by exploring the identification systems in Ghana, and two OECD countries; Denmark and the United Kingdom, through literature review and my real life experiences of staying in those countries. The choice of exploratory case study at this initial stage of my study is in consonance with Yin, (2011), thus studying the phenomenon in its real life context, especially where there is an unclear boundary differences between the phenomenon and context (Yin, 2011a). Scientific research on user-centric identity and trusted identity management within the context of a nation are in the trial stages (Bertino, 2012; Grant, 2011a; IBM, 2010; Microsoft, 2011).

Moreover the choice of exploratory case study was very necessary since it is the most appropriate strategy for resolving a "what" question was the case and hence a justifiable rationale for conducting an exploratory study. Literature and document review, interviews and quasi statistics method in the form of citizens' perception survey were the means adopted for data collection.

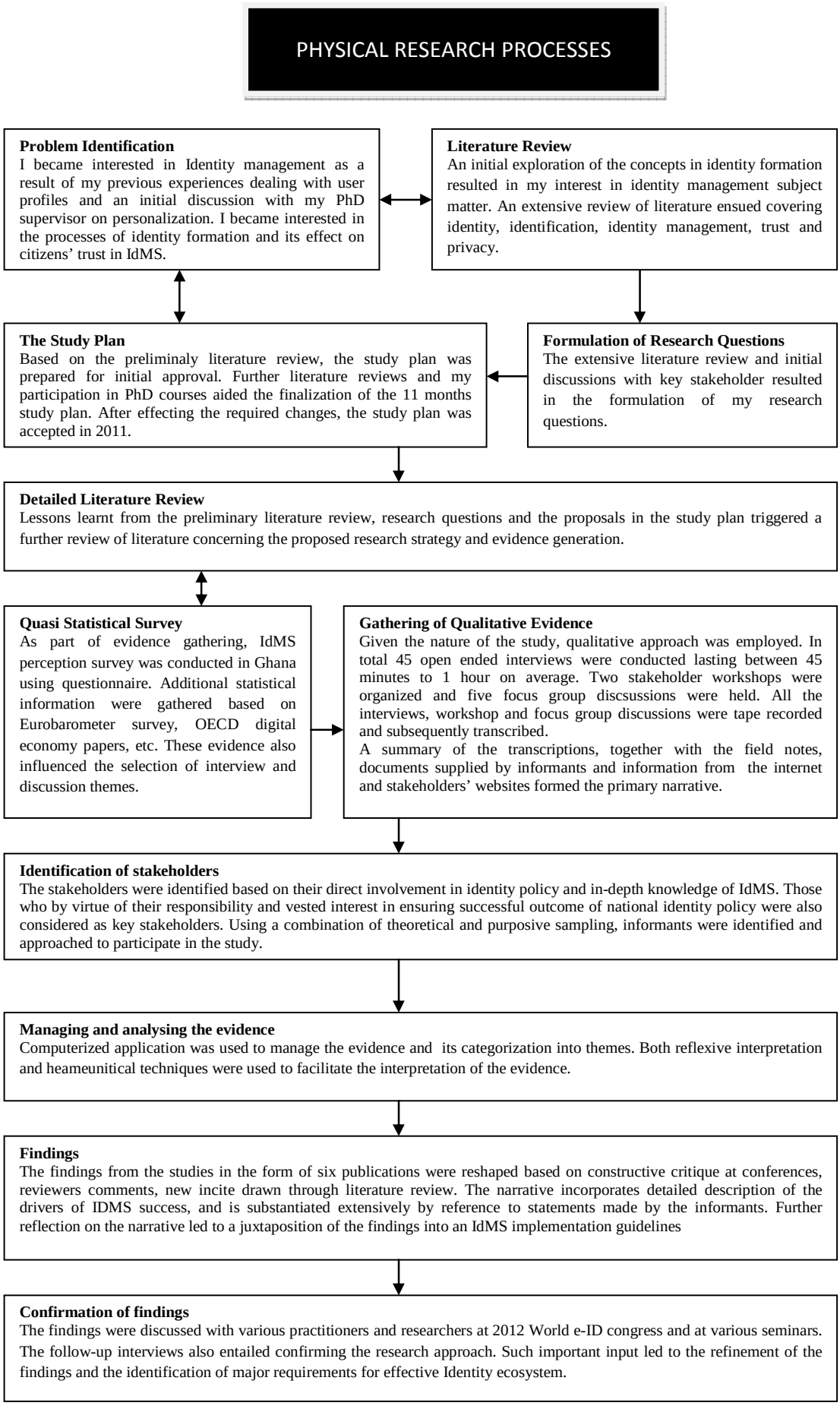


Figure 26 Actual Research Audit Trail.

Phase 2 was an attempt to identify the causes of the identification challenges as revealed in the findings from Phase 1. The strategy adopted for this inquiry is the explanatory case study of identity management systems in Ghana using triangulation as a research strategy. Explanatory case study strategy is very useful when the inquirer seeks explanation using "how and why" research questions (Yin, 2011a). Such questions are necessary in dealing with operational links that need to be traced over time (Yin, 2008a) The major sources of data collection at this stage were; interviews, focus group discussion and the stakeholder workshop/seminar.

Phase 3 The strategy adopted for the final phase of the study is a confirmatory case study which integrates the result from the first and second phase of the study in addition to further evidence from stakeholder workshop, focus group discussion and a series of interviews. The selection of stakeholders was based on the preliminary study of stakeholder theory and analysis (Crane & Ruebottom, 2012; Edward Freeman, 2010) as specified in Chapter 3. Stakeholder theory is concerned with who has input in decision making as well as the beneficiaries from the outcomes of such decisions (Phillips et al., 2003, p. 487).

Thus the stakeholders were categorised as direct and indirect. The direct stakeholders comprised of institutions that are directly involved in the issue of identity credentials, and enforcement identity policies in Ghana as shown in Table 4. The indirect stakeholders include institutions that rely on the identity credentials to facilitate business transactions.

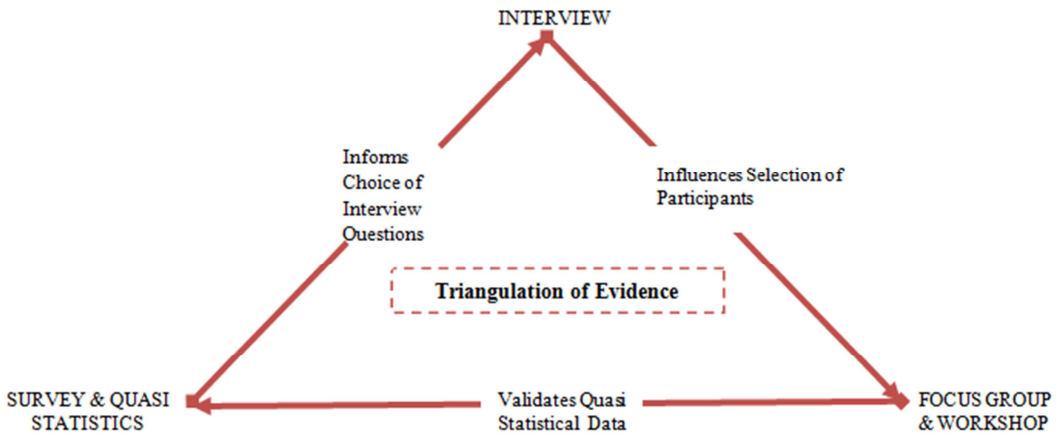


Figure 27 Triangulation of Evidence.

4.4.2 Unit of Analysis

The study focused on national identity management systems and how they can be trusted and citizens centered. The unit of analysis are the citizens and the key actors who have a stake in the crafting of national identity policies. The stakeholder analysis gave me a broader perspective on how identity management can be trusted and citizens centered given that these stake-

holders can give meaning to their perception and these meanings actually influence their practice. The nature of my research questions gives credence to the nature of research strategy and is key to finding the best approach to crafting trusted and citizen centered identity management systems.

4.4.3 Sources of evidence

Qualitative research using a case study as a research strategy thrives on the rich source of evidential knowledge that is provided from multiple sources, where the complexity of the unit is studied intensively (Yin, 2011a). In compliance with such requirements, the goal was to obtain a rich set of data surrounding the research objective and the related research questions, and to capture all the contextual realities and complexities (Benbasat, Goldstein, & Mead, 1987; Cavaye, 2008). The key sources of evidence were as follows:

Focus Group

The focus group method is a qualitative data gathering technique where focus group sessions involve a group of participants assembled for a planned discussion to explore a specific topic of interest to researchers in a permissive, non-threatening environment (Krueger & Casey, 2009). Focus groups are an organized discussion group that capitalizes on communication between participants in order to gather as through the group interaction (Gibbs, 1997; Kitzinger, 1995a, p. 311). The focus group research method benefits from the interaction among participants, which can reveal shared ideas, reactions, and opinions on the topic of the study. The unit of analysis of a focus group is not the members but the group.

Focus groups provide the opportunity for the inquirer to collect in detail, qualitative data about a particular product, concept or innovation in an interactive manner in order to reveal differing viewpoints and perspectives among the participants (Jamieson & Williams, 2003). It is thus, a powerful and flexible means to gather qualitative evidence by exploring participants' opinions, ideas or attitudes especially where group interaction is sometimes the ability to revise individuals' initial perceptions and opinions (Gibbs, 1997; Kitzinger, 1995a, p. 311). These structured process of interaction aid the formation of perceptions and attitudes, in a sequential series of one–on–one interviews with the same individuals (Krueger & Casey, 2009). Moreover, the objective of a focus group is the group interaction and not for group decision making, consensus building or to provide recommendations as is the case of group participatory methods like Delphi method (Kitzinger, 1995b). Thus, a focus group facilitator must create a permissive environment that nurtures different perceptions and points of view without needing to reach consensus. The extensive literature on focus groups recommends that groups should be composed of at least six participants, with most authors proposing be-

tween five and twelve participants as the ideal number (Morgan, 1997). Very large focus groups can be unproductive as it may be difficult to include contributions from all participants and there may be a tendency for the discussion to fragment and a series of mini–conversations to emerge (Krueger & Casey, 2009). Very small focus groups are unlikely to reveal significant insights from the group process as they can effectively become a series of individual interviews.

Characteristics	Academic/ Research	Financial Institution	Media	Technology	Identity Providers	Policy Makers	Security Agencies	Other	Total
Number of Participants	7	3	5	5	10	7	3	5	45
Female Participants	1	0	1	1	1	1	1	2	8
Male Participants	6	3	4	4	9	6	2	3	37
Focus Group 1	1	1	1	1	2	2	1	1	10
Focus Group 2	1	1	1	1	2	1	1	1	9
Focus Group 3	1	1	1	1	2	1	1	1	9
Focus Group 4	2	0	1	1	2	1	0	1	8
Focus Group 5	2	0	1	1	2	2	0	1	9

Figure 28 Characteristics of Focus Group Participants.

Interviews

A series of interviews were conducted during all the three phases of the study. I adopted serial interview (Murray et al., 2009) with open ended interview questions that usually give room for further discussions (Yin, 2008a). Each interview lasted between one hour and one and a half hours. Interviewees were chosen in a purposive manner, rather than randomly, in order to assure extensiveness and diversity of opinion regarding the use of identity management systems and national identity policies. This style of Interviewing has the added advantage of revealing certain important facts about the interviewees and the context such as languages, social cues, opinions, attitudes, beliefs and feelings (Yin, 2008a).

It also offered interviewees the opportunity to clarify some of the points raised during the workshop to solicit for further information. Interviewees included the officials of identity issuers, policy makers, journalists, private businesses involved in identity verification, and identity card manufacturers. This activity is also a very good way of establishing a good relationship with key stakeholders which acted as a means of identifying other important stakeholders that I might not have included in my initial list of interviewees. The following issues were considered during the interviews:

- Interviewees are given a brief explanation about the purpose and format of the interview to be conducted.
- Participants were given prior information about the length of the interviews. The duration of all the interviews were between forty-five minutes to one hour.
- Where appropriate, the interviews were captured on a digital voice recorder with use being made of hand-written notes either as a complement to the recorder or as an alternative.
- Permission was sought from interviewees prior to the voice recording of the interviews and assurances were given regarding confidentiality.
- Interviews were tracked by keeping a log of where and when the interviews took place and who took part in the interviews.

Stakeholder Workshop

Problem Structuring Method (PSM) have suitable in multi-actor situations, and their characteristic mode of operation is the workshop, in which representatives of stakeholding groups interact. In such an environment, commonly fragmented information and knowledge could be organised and synthesised through a carefully formulated discussion questions. The organisers and the facilitator of the PSM must provide an environment in which this can happen effectively. Thus, how the workshop is established and its processes managed can be crucial to the success of the engagement.

To achieve the desired goal, the facilitator must ssume the positon of a disinterested facilitator, and allow participants to have their voices heard. This involves managing the disparate contributions and making the participants feel safe in expressing their views as fully and openly as possible. Thus skilful communicator is not the key requirement, but rather sensitivity to potential fears and anxieties of participants. and to the power relations which may inhibit free expression (Phillips and Phillips, 1993; Ackermann, 1996; Vennix, 1996.)

A stakeholder workshop was organised in Ghana on January 16, 2012, at Ghana Technology University College (GTUC) in Accra. 75 participants were offered the opportunity to discuss a number of issues and listen to presentations highlighting issues concerning secondary uses of personal information. Letters were written to all participants and participating institutions, and detailing the theme, agenda and activities for the day.

The participants were made up of senior officials from national institutions involved in the collection and storage of personal information, such as the Registrar of Births & Deaths, The Passport Office, Driver and Vehicle Licensing Agency (DVLA), National Identification Au-

thority (NIA), the National Health Insurance Authority (NHIA), the Electoral Commission (EC), the Ghana Revenue Authority (GRA). Also represented were senior officials of the major financial institutions, biometric and identity-related businesses, academic institutions, the media, non-governmental organisations involved in civil right advocacy, and the general public. Ghana was selected as the research setting because the challenges faced by the economy with respect to identification and secondary uses of personal information are similar to those of other developing countries. Notable challenges include unreliable civil registration systems, electoral issues due to unreliable voters register, lack of identity management systems interoperability, etc.

The workshop began with a statement from the Minister of Communication and a keynote address by the President of GTUC, who chaired the event. To inform discussions, participants were given background information and copies of the discussion questions during a presentation on privacy and identity management. The presentation highlighted the key concepts of identity management, including major policy, technological and regulatory issues and related IdMS research and practices in OECD countries. This was followed by another presentation on existing secondary uses of personal information for identity verification by financial institutions. After the presentations, participants shared their observations on the topic during the discussion session. The facilitator's role was to keep the discussion focused on the problem at hand and prevent the participants from engaging in personality-oriented conversation (Papamichail et al., 2007).

Participants were also made to discuss the issues raised and share their experiences and their reservations. Where particular issues or questions were sector-specific, the agencies concerned were given the opportunity to respond to such questions. Some of the discussion questions were:

1. What are the potential benefits and risks regarding the secondary use of personal information?
2. Who has the right to access personal information held by government agencies and for what purposes?
3. What are the evolving public trust issues with respect to secondary use of personal information?
4. Do citizens have the right to put constraints on the use of their personal information?
5. What problems may develop as innovative technologies enhance the ability and ease of widespread personal data sharing for a secondary purpose and commercial uses?

6. What can be done to address issues arising from inappropriate use and/or exploitation of personal information?
7. What regulations, legislation, and/or policies and procedures are needed to address these issues?

Characteristics	Academic/ Research	Financial Institution	Media	Technology	Identity Providers	Policy Makers	Security Agencies	Other	Total
Number of Participants	7	3	5	5	10	7	3	5	45
Female Participants	1	0	1	1	1	1	1	2	8
Male Participants	6	3	4	4	9	6	2	3	37

Figure 29 Characteristics of Workshop Participants.

4.4.4 Secondary Data Sources

This study draws from two major secondary sources of evidence, in the form of scholarly publications, industry reports, reports issued by international agencies, and participation in PhD courses. OECD Digital economy papers, statistics from World Economic Forum, publications of European Union (EU) Privacy and Identity Management research consortia and newspaper and organisational publications in Ghana and Africa. These sources immensely influenced the definition of research context, the design of interview guide, focus group and stakeholder workshop questions and in all publications during the study. The secondary sources of evidence also impacts on the discussions and analysis of the research findings and the conclusions drawn.

Scholarly Publication: Although discussions on privacy and identity have been ongoing for many years, the concepts as used in digital identity management is fairly new. There were also not many studies on the application of IS success theory in the assessment of IdMS effectiveness or success. This implied broadening the scope of the research to cover the electronic government, which like an umbrella domain within which national identity management is situated. In the course of the study, I witnessed a dramatic increase in Identity management literature with respect to the technical development and various proposed applications for privacy enhancing.

However, I observed that not many research were being conducted on societal aspects of identity management. For instance, a search on Google scholar with the following parameters *"successful national identity management systems", or "successful identity management systems"* revealed nothing but "*successful e-id*" brought only one hit. However, changing the

parameters to “successful e-government” made 1,560 hits. Similarly *“national e-id”* or *“national electronic ID”* revealed between 65 to 69 hits. Interestingly replacing the keyword “successful” with “effective” as follows "effective identity management systems", made 5 hits, all of which discussing effective IdMS within the context of an organisation.

With effectiveness or success of an information system in general, it is interesting to find several literature, that sought to clarify the dependent variable in IS Success, testing and respecification of the DeLone and McLean IS success model (Eom & Stapleton, 2011; Mun, Yun, Kim, Hong, & Lee, 2010; Petter et al., 2012; Sharkey, Scott, & Acton, 2010; Tona, Carlsson, & Eom, 2012; Urbach & Müller, 2012). Such studies have informed my understanding and the development of my trust framework.

Statistics and Official Reports: This study has also been influenced by various reports by OECD Digital Economy Papers and statistics from various international agencies like Euro Barometer Survey, UNESCO, etc, and quasi statistical survey conducted in Ghana.

PhD Courses and **Conferences:** Participation in various PhD courses immensely broadened my horizon of understanding of academic research and academic writing. In particular, courses on the Political Economy of ICT and Techno-economics of ICT provided a very good historical background on ICT development and the role of institutions and its implication on contemporary developments in information and communication technology. Similarly, the courses on Theory of Science and Academic writing, Qualitative Research helped me to appreciate the historical background of the various philosophical paradigms and their implication on scientific research and practice.

Participation in the Academic Writing course also enriched my understanding of the rudiments of academic writing and publication of research in academic journals and conferences. I also learnt insightful lessons during my participation in various conferences and workshops. Particularly, participating and presenting a paper at the world e-id congress gave me more insight into various cutting-edge technologies and the state-of-the-art on privacy–enhancing IdMS and trusted Identities identity management systems. I also had the opportunity to discuss pertinent issues with many of the participants.

E-mails, Skype and Podcast: In the course of the study, I exchanged several e-mail and Skype conversations with various stakeholders and IDM researchers. Given the distance barrier, e-mail and Skype have proven to be a very good means of communication and seeking clarifications on pertinent questions and also a very good means of keeping track of research data. This is notwithstanding the context and unobtrusive nature which ensures convenient interaction and their ability to offer asynchronous means of interaction.

E-mail is also a very good means of obtaining documentations and reports from various organisations, as it is also a rich repository of relational communication and thus allows writers the flexibility to personalize their messages. This suggests that e-mail can assist in a negotiated understanding between the email sender and the recipient since the recipient can seek clarifications on a particular subject. This interactive characteristic of e-mail and particularly, Skype makes it somehow similar to face-to-face communication, whilst retaining its asynchronous nature. Thus it allows writers to compose, edit and send it at their convenience (Tidwell & Walther, 2002; Z. Wang, Walther, & Hancock, 2009).

Project Phase	Type of Fieldwork	Location	Activity	Approach	Characteristics of Participant
1	Fieldwork 1	Ghana	IDMS perception Survey	501 Questionnaire were circulated	A group of MBA students from West Africa, Young Adults in three major cities in Ghana - Accra, Tema and Kumasi, and general public.
1	Field work 2	Ghana	Interviews	20 open-ended Qualitative interviews in ten days	Interviewees included; key officials of credential issuers, financial institutions and general public.
2	Field work 2	Ghana	Workshop 1	Stakeholder workshop in GTUC, Accra on secondary use of personal information	Participants included; Credential issuers, financial institutions, IT organsiations, academic institutions, Media, private businesses, policy makers and NGOs.
2	Field work 2	Ghana	Expert Interviews	25 open ended interviews were arranged in 20 days	Interviewees included all major stakeholders in the Ghanaian identity ecosystem.
3	Field work 2	Ghana	Workshop 2	Second Stakeholder workshop in GTUC, Accra which focused on crafting a trusted identity policy guidelines	Participants included; Credential issuers, financial institutions, IT organsiations, academic institutions, Media, private business and policy makers, NGOs, students from various schools and the general public
3	Field work 2	Ghana	Focus Group	5 Focus group sections were organized in Accra	Participants included a blend of people from diverse background. Group sizes ranged between 9 to 11.Each group had both male and female participants.

Table 12 Overview of Empirical Data Collection.

4.4.5 Data Interpretation

What we call our data are really our own constructions of other people's constructions of what they and their compatriots are up to (Geertz, 1973).

The data collected from primary and secondary sources were mainly made up of text, statistics, charts, voice and video recordings, notes and images that transmit ideas and concepts. In consonance with the overarching objective of the study, data collection interpretation was significantly informed by philosophical constructivism. This world view takes the position that our knowledge of reality, including the domain of human action, is a social construction by human actors. In that sense, what I call my data in this study are in fact my own constructions of other people's constructions of what they and their compatriots are up to (Geertz, 1973, p. 9; Walsham, 2006). In his paper titled;"*interpretive case studies in IS research"* Walsham, (1995) also observed that the quality of researchers' construction of reality (data collected) hinges on a good theory and an insightful analysis (Walsham, 1995). Thus, the interpretation of data and the drawn conclusion follows what is described as the hermeneutic circle (Heidegger, 1982; Warnke, 2011). Thus an understanding of the text as a whole is established by reference to the individual parts and similarly understanding of each individual is achieved with reference to the whole.

In this study, data is interpreted and analysed, in the light of the theoretical underpinning presented in Chapter 3. Such an interpretivist posture implies that texts are perceived as the media that transmit experiences, beliefs and judgements of the author on the interpreting subject.

Additionally, in my interpretation of the data and the phenomena, I see my role as an involved researcher through participant observation and not an action researcher (Walsham, 1995). The data analysis and interpretation were partly conducted during the three phases of the research. In interpreting transcripts of voice recording, notes and other written data, I observed the fact that the literal meanings are within the text, which is detached from emotions and communication mannerism (Gadamer, 1975, p. 392). Detailed analysis of the findings is presented in Chapter 5.

Phase	Objective	Theoretical Reference	Data Collection method	Type of Instrument	Focus
1	Explore the factors IDMS uses in developing countries	Davis	Interviews and Questionnaires used for	Open ended interviews	Factors that influence effectiveness of Identification systems
1& 2	To understand the relationship between individuals' intentions to disclose personal information, their actual personal information disclosure behaviours.	(Roger C. Mayer, Davis, & Schoorman, 1995b) (K. Cameron & Jones, 2007)	Interview and Secondary sources	Open ended Questions	Analysis of Privacy-Enhancing Identity Management Systems
	To understand the major issues involved in the design of privacy-enhancing IDMS and contribute to improved framework and design principles.	(Roger C. Mayer et al., 1995b) (K. Cameron & Jones, 2007)	Interviews and Secondary sources	Open ended questions	Keeping Identity Private; Establishing Trust in the Physical and Digital World for Identity Management Systems
2	To provide a means of communicating identity-related concepts to policy-makers, users and technologists.	(Pavlou, 2011b), Stakeholder theory (Crane & Ruebottom, 2012; Donaldson & Preston, 1995; Jones & Wicks, 1999)	Interview, Workshop Secondary sources	Open ended questions	Secondary Uses of Personal Identity Information: Policies, Technologies and Regulatory Framework
2	To understand the key stakeholder concerns regarding the collection, storage and use of personal information and how such concerns should be addressed to ensure trusted identities.	(Delone & McLean, 2003; Petter et al., 2008, 2012).	Interview, Workshop Secondary sources	Open ended Questions, Problem structuring method	Building Trusted National Identity Management Systems – Presenting Privacy-Concern Trust Curve
2	To identify the key requirements for crafting a trusted identities ecosystem	Problem structuring methods (Papamichail et al., 2007; Sinkko et al., 2008) Stakeholder theory	Interview, Workshop Secondary sources	Open ended questions	Towards a Trusted National Identities Framework

Figure 30 Theoretical References and Sources of Evidence.

Chapter 5 Findings and Contributions

The key findings, contributions and limitations of this study are presented in this chapter based on six research papers published in the course of the study. Three of the papers were published in peer reviewed academic journals and the remaining three were published in proceedings of peer reviewed academic conferences. A summary of the published papers is shown in Table 13.

An overview of the papers is first presented, followed by the level of publication, and the overarching research question(s) that the paper addresses. The relevant research questions and objectives in Chapter 1, to which a paper relates is also discussed. The findings from each of the studies, a summary of contributions to research and practice, and the major limitations of each of the studies are also discussed. The following are highlights of the main findings discussed in each of the papers presented in this thesis.

Paper 1 discusses identification systems from the perspective of a developing country focusing on the major factors that influence effective uses of IdMS by citizens. The findings indicate that although the introduction of identification systems by governments are usually mandatory and are sometimes coercive in its introduction, citizens' trust in the system and the institutions are sometimes a major precondition for its take-off. This study did set the scene for my further studies on trust and privacy as described in sections of subsequent papers.

Papers II and III explore the factors affecting citizens' attitude towards IdMS and their intentions to disclose personal information, and its effect on the development of privacy-enhancing identity management policy. Various privacy enhancing IdMS research and initiatives were reviewed with respect to their implications for national identity management policy.

Paper IV discusses how to effectively communicate identity-related concepts to policy-makers, technologists, credential issuers and other stakeholders. The paper addresses the core issues in relation to secondary uses of personal information based on results from a stakeholder workshop in Ghana and a series of interviews. The paper also explains what constitutes personal identity information and user concerns in relation to secondary uses of personal information. Particularly, we observe the dimensions of information privacy and how they influence citizens' confidence in credentials and credential issuers. It is at this stage that we learn the privacy concerns from citizens, institutional perspectives and the state-of-the-art in trusted IdMS research and practices.

Paper V also discusses the key requirements for building a trusted National Identity Management Systems. The Privacy-Concern Trust model is introduced at this stage.

Finally, paper 6 describes the requirements of the trusted identity ecosystem, which is a critical enabler for effective uses of digital IdMS. The findings show that, beyond the threshold level of trust, societal information privacy concern is low; and trust is high, thereby encouraging further institutional cooperation and citizens' informational self-determination. The table below presents a summary of the various research papers presented in the thesis.

Paper	Author (s)	Title	Publication Level	Research Question Addressed
1	Adjei & Tobbin	Identification Systems in Africa; The Case of Ghana	Published in proceedings of the 12th International Symposium on Information Science (ISI 2011), 9 - 11 March 2011, Hildesheim. (Internationales Symposium für Informationswissenschaft, Hildesheim, 9.—11. März 2011)	Research Question 1: What underlying factors motivate or inhibit IDMS implementation
2	Adjei & Olesen	Analysis of Privacy-Enhancing Identity Management Systems	Published in Proceedings of WWRF26-WG1-xx	**Research Question 1:** The major issues involved in the design of privacy-enhancing IDMS and contribute to improved framework and design principles for
3	Adjei & Olesen	Keeping Identity Private; Establishing Trust in the Physical and Digital World for Identity Management Systems	Published in IEEE Vehicular Technology Magazine September 2011	**Research Question 1 and 2:** The major issues involved in the design of privacy-enhancing IDMS and contribute to improved framework and design principles for these
4	Adjei & Olesen	Secondary Uses of Personal Identity Information: Policies, Technologies and Regulatory Framework	Published in *Digiworld Economic Journal*, no. 88, 4th Q. 2012, p. 79.	Research Question 2 and 3: - What underlying factors motivate or inhibit IDMS implementation - How can government agencies justify the implementation of national identity management systems.
5	Adjei & Olesen	Building Trusted National Identity Management Systems – Presenting Privacy-Concern Trust Curve	Published in Proceedings of Centric 2012	Research Question 2 and 3: How can government agencies justify the implementation of national identity management systems?.
6	Joseph K. Adjei	Towards a Trusted National Identities Framework	Accepted for publication in Info Journal Emerald	Research Question 2 and 3: What architectural framework will ensure citizen centric national identity management systems?

Table 13 Summary of Published Papers.

5.1 Paper Selection

A careful consideration is given to the papers selected based on their relevance and contributions to addressing the various research objectives outlined in Chapter 1. Together, the six papers contribute to the theory building from a qualitative research background, in consonance with the methodological paradigm approached in this study, and presented in Chapter 4. The papers are also a reflection of my appreciation of the trusted and citizen centric identity management phenomena based on the application of different analytical methods and interpretative cycles.

The papers are numbered from 1 to 6 in the order in which the papers were written to aid referencing in the discussion of findings. The progression of the papers also provides an indication of the research progress and the hermeneutic circle – which is described in section 4.4.5 of chapter 4. Thus, the papers reveal how an understanding of the phenomenon of interest was refined and enhanced during the research. Chronologically, some of the concepts and processes are carried over in their refined form.

5.2 Identity Management in Africa; The Case of Ghana

Paper 1 is based on a preliminary quasi statistical data collection collected during the early stages of the study, and analysis of existing literature. Using IdMS in Ghana as a case study, this paper examined the effects of perceived usefulness and ease of use on IdMS effectiveness and concluded that trust and privacy concern play major role in IdMS uses. The results also showed that citizens perceptions and experiences can unduly affect IDMS uses. During this initial phase, it also became apparent that user awareness of technology, institutional issues, trust and privacy concerns are major factors affecting identity management effectiveness. The paper also described at a conceptual level, what deliberations have to be taken into account to come up with appropriate compromises in the implementation of national identity management systems.

5.2.1 Research Objective & Methods

This paper addressed my first research question as described in Section 1.3.2 in Chapter 1, under the phenomena of interest. The objective was to identify the key factors that determine the effectiveness of national identity management systems. The goal was to outline the critical factors that policy makers must consider in implementing an effective and efficient IDMS. The study was based on an extensive literature review, interviews and a quasi statistical survey about citizens' perceptions of identity management systems.

5.2.2 Research Findings

An interesting finding was that majority of the respondents prefer that identity cards be issued to citizens free of charge as a means of universal coverage and forgery prevention. Respondents also believed that their interest would be considered in deciding how identity data is used which is consistent with Davis' (1989) suggestion that the design characteristics of a system exert immediate effects on perceived usefulness as well as indirect effects via perceived ease of use. However, a follow-up interviews of some of the respondents revealed an opposite results which is an indication that respondent did not adequately appreciate the survey questions. This outcome reinforced my resolve that, a qualitative research approach, using problem structuring methods will be the best approach to the study.

5.2.3 Contributions

This study contributes to IdMS research by enriching our understanding of the best approach to engage citizens regarding their perceptions on national IdMS. It also adds developing countries dimension to IDMS research. The study is also an important source of reference regarding factors that affect citizen adoption of IDMS. It also shows that beside perceived usefulness and ease of use, institutional cooperation, and perceptions of trust and privacy concerns must be taken seriously.

5.3 Analysis of Privacy Enhancing Identity Management Systems

Following the results from the paper 1, this paper explored the literature on privacy, trust, contemporary initiatives in that regard, and how businesses use identity information. This study is an attempt to understand the relationship between individuals' intentions to disclose personal information, their actual personal information disclosure behaviours, and how these can be leveraged in the development of privacy-enhancing identity management systems. Thus the concepts of privacy, trust, and the key regulatory and research initiatives on privacy enhancing IDMS were also explored specifically the Laws of Identity, the Fair information practice principles (FTC, 2000; Rotenberg, 2001; Schwaig, Kane, & Storey, 2006; Schwartz, 2000) and the Privacy by Design principles (Cavoukian, 2012) and OECD Guidelines on privacy (OECD, 2002, 2011a).

5.3.1 Research Objective & Methods

The objective of this study is to understand the major design considerations for privacy-enhancing IDMS and to contribute to an improved frameworks and identity management systems design principles. To achieve these set goals, the paper analysed the existing international privacy regulations and the proposed standards and best practices on trust and privacy. This

study draws extensively on literature, testing and demonstration of various IdMS applications as a means of gaining deeper insight into privacy enhancing IdMS.

5.3.2 Findings

The study unravelled the fact that identity management systems that facilitate anonymity and pseudonymity may offer better promise of privacy. Similarly, it was established that linking identities that do not share the same degree of anonymity, or that contain different sets of attributes may allow others to overcome pseudonyms and discover the user's identity. The analysis also revealed that, controlling linkability require the segregation of different contexts such that observers are unable to accumulate sensitive data.

Moreover it was established that users' perceptions of privacy and trust must be taken seriously in order to adequately derive benefits of identity management systems. Lastly, the study also highlights the need for more study on establishing trust in the physical world since the mechanisms of establishing trust in the physical world are not necessarily the same as those that are used online.

5.3.3 Contributions

This study provides important identity policy guidelines for practitioners and policy makers by highlighting the identity practices in data collection, use, and retention that can be left to market forces and those that should be the subject of government interventions. The study also contributes to the discussions on the best way of resolving the "Privacy Paradox" and the dilemma between privacy and identity assurance. This knowledge is very important for identity policy formulation since it has implications for institutional cooperation and citizens' ability to exercise informational self determination. Thus this study also contributes to IdMS research by adding to existing knowledge of IdMS.

5.3.2 Limitations

The key limitations of this study were that the study relied mainly only on secondary sources and also did not explore how the principles and technologies specically address privacy and trust issues. Subsequent studies such as papers 4 and 5 addressed these limitations.

5.4. Keeping Identity Private

This study is an attempt to understand the relationship between individuals' intentions to disclose personal information, their actual personal information disclosure behaviours, and how these can be leveraged to develop privacy-enhancing identity management systems that users can trust. Legal, regulatory and technological aspects of privacy and technology adoption are

also discussed. The study draws on three streams of literature, namely technology adoption, trust and privacy-enhancing IDMS. Thus this paper is a further improvement on paper 2.

5.4.1 Research Objective

The objective of this paper was to understand the major issues involved in the design of privacy-enhancing IDMS and contribute to improved framework and design principles. This study is also important because it offered me the opportunity to summarize the literature that is available on privacy enhancing IDMS. This is consistent with the fundamental principle of all qualitative research approaches which is to explore meaning and develop understanding of the research topic (Aveyard, 2010). This conceptual paper addresses our first research question. The paper also based on the premise that designing a privacy-enhancing technology is not only a technological problem, but has theoretical, social, and regulatory dimensions must also be addressed. The research problem addressed in this paper is *"what factors must be considered in designing privacy-enhancing IDMS that address both online and face-to-face identity management issues?"*

5.4.2 Methods

This study also complements the previous study which focused on reviewing the central theoretical themes in privacy-enhancing IDMS, trust (Roger C. Mayer et al., 1995b) and citizens' acceptance of IDMS Technology (Fred D. Davis, 1989). These conceptual understandings formed the basis of the analysis of key regulatory and research initiatives on privacy-enhancing IDMS. This is a conceptual paper, therefore no empirical data were gathered but rather, also formed the basis for subsequent research as presented in subsequent studies. We thus identified the key concepts and propositions which were used to represent or describe (but not explain) the process of keeping identity private. In effect the propositions identified in the models are logical statements rather than epistemological relationships (Meredith, 1993). The paper begins with a review of the related literature and then based on the understanding of the literature, made recommendations on policies, technological and regulatory framework for keeping identity private.

5.4.3 Research Findings

The key regulatory and research initiatives on privacy-enhancing IDMS such as the Laws of Identity (K. Cameron & Jones, 2007), the FIP principles, and the PbD (Cavoukian & Carter, 2006) principles were examined. The findings indicate that to ensure that national identity management systems are privacy enhancing, the systems must be useful, easy to use and must observe privacy and trust requirements. We also observed that adherence to such design prin-

ciples and guidelines can contribute to resolving the privacy paradox (Norberg et al., 2007) and the dilemma between privacy and identity assurance (C. H. Lee & Cranage, 2011). Another observation made in this study is the fact that identity providers and policy makers unduly equate secrecy to privacy and thus fail to address legitimate concerns of key stakeholders in identity management. It was also observed that the underlining reason driving privacy-enhancing IDMS is to enable the users to prove a predicate of their identity without giving third parties the opportunity to access unwarranted information.

5.4.4 Contributions

An interesting aspect of the study lies specifically in its contribution to theory developments in privacy-enhancing IDMS, and technology adoption in general. The study also contributes to the consolidation of the disparate and disjointed design principles and guidelines in order to empower users, protect their privacy, and support fine-grained control of access to resources online. By adding perceived privacy and trust as constructs in acceptance of IdMS, the study contributing to the ongoing discussion on effective ways of implementing privacy-enhancing IDMS. The paper also clarifies the role of the guidelines and regulatory framework on privacy enhancing IDMS. For instance, we offer key factors that need to be considered in the implementation of privacy-enhancing IDMS. This paper is an important contribution to research and the development of design guidelines for privacy-enhancing IDMS.

5.5 Secondary Uses of Personal Identity Information: Policies, Technologies and Regulatory Framework

This paper is based on the results of a stakeholder workshop and interviews in Ghana on secondary use of personal information. Although personal identity information must primarily be used for protecting and promoting the physical needs of individuals, it has also become central to the business models of the digital age due to its use for other secondary purposes, resulting in various innovative identity management (IdM) solutions in OECD countries. Nonetheless, developing countries were still not able to address basic identification challenges such as civil registration, real-time credential verifications, etc.

5.5.1 Research Objective

The objective of this paper is to provide a means of communicating identity-related concepts to policy-makers, technologists, privacy advocates and users. The paper also addresses core issues relating to what constitutes personal identity information and user concerns in relation to secondary uses of information. The study proposes the adaptation and application of exist-

ing IdM research and experiences from OECD countries to deal with issues involved in using personal information for secondary purposes in developing countries.

5.5.2 Methods

This paper adopted a qualitative methodological approach for data collection (Yin, 2008a, 2011a) resulting in a review of literature on the state-of-art on identity management, privacy issues in secondary use of personal information. The primary data for this paper consists of responses of a series of interviews and a stakeholder workshop organised in Ghana. Interpretative Phenomenological Analysis (J. A. Smith, 2004) approach was applied in the data analysis due to its reliability with respect to audio-visual contents, which is very common in focus group and workshop discussions. A stakeholder workshop offered participants the opportunity to discuss a number of issues and listen to presentations highlighting issues concerning secondary uses of personal information. Ghana was selected as the research setting because the challenges faced by the economy with respect to identification and secondary uses of personal information are similar to those of other developing countries. Notable challenges include unreliable civil registration systems, electoral issues due to unreliable voters register, lack of identity management systems interoperability, etc.

5.5.3 Research Findings

The discussions and interview responses revealed the need for a paradigm shift with respect to ownership and control of personal information. It was observed both from literature and the discussions and responses from the workshop and interviews that, individuals seek not just to assert the identity and privacy of their physical being, but an informational representation of the chain of their life events that define who they are. Thus a particular event of relevance depends on those with whom the individual is interacting which must lead to different entitlements. In that regard, attention must be focused on access to and control of personal information rather than data ownership.

The workshop therefore recommended focus on data access, control policies and practices as the best approaches to risk management and mitigation for illegitimate secondary uses of personal information. Another interesting finding that emerged from the discussions and the responses is a lack of understanding and inability to differentiate privacy from secrecy; and secondly, inadequacy of safeguarding procedures that address user concerns in relation to secondary uses of personal information. In essence, citizens would like to be able to assert their identity with ease and confidence and hence they need such assurances (Crosby, 2008a). The workshop also observed that lack of clear regulations on secondary uses of personal information could result in the erosion of public trust.

5.5.4 Contributions

Central to effective uses of personal information is an efficient civic registration system, a regulatory framework that encourages institutional collaboration, clear policies and guidelines that provide assurance of citizens' privacy and cost effective application identity management systems. This is what the paper attempted to highlight by using the stakeholder approach and is considered its major achievement. Moreover, the use of the stakeholder workshop was as an attempt to bring together users and researchers, public and private sector organizations. It is a key methodological contribution and also a response to (F. Bélanger & Crossler, 2011) call for closer collaboration between researchers, developers and users to ensure effective uses of privacy enhancing identity management systems.

The study has also helped to raise awareness of current technological developments in IdMS and how developing countries can adapt and apply some of the relevant principles. The study has also shown that the application of digital identity management is a process, rather than a state. Thus, the integrity of the process hinges on: how reliable were the initial processes of registration, verification and enrollment, and how hard is it to duplicate or alter the credentials used? (Wilton, 2008a).

5.5.5 Limitations

Like many qualitative research methodologies a key limitation of our study is its lack of empirical testing of the claims compared to quantitative research. Also given that certain societal dynamics are peculiar to different countries, care must be taken in generalizing the findings from our study to other countries. However some of the limitations are ameliorated by the extensive review of related literature.

5.6 Building Trusted National Identity Management Systems – Presenting Privacy-Concern Trust Curve

This paper discusses the effect of trust and information privacy concerns on citizens' attitude towards national identity management systems. It also introduces the privacy-concerns-trust model, which highlights the role of trust in mediating and moderating citizens' attitude towards identity management systems.

5.6.1 Research Objective

The objective of the study is to explain to identity policy makers and other key stakeholders the requirement for achieving the trust threshold. It also shows how stakeholders information privacy concerns regarding the collection, storage, use, and transmission of personal identity information (Bennett & Raab, 2003a), should be addressed to ensure trusted identities. This

study also draws on literature on trusted identity initiative by the government of the United States (Grant, 2011b).

5.6.2 Methods

This study entailed two main phases – an exploratory phase, which saw the development of the model based on literature, and a qualitative based confirmatory phase, which was used to evaluate the model. The conceptual model on the basis of theoretical considerations is part of an on-going research project that seeks to present a reliable and valid instrument for measuring trusted identities ecosystem. The exploratory phase of the study was organized in line with two-step approach for operationalizing constructs and identifying measures (Burton-Jones & Straub, 2006). Due to the multi-stakeholder nature of trusted national identities, we decided to adopt a research approach that engages the key actors and hence a qualitative methodological approach was deemed the most appropriate means for data collection from a societal perspective (Creswell, 2007a; Yin, 2011b). We also applied interpretative phenomenological analysis (J. A. Smith, 2004) in data analysis because of its usefulness in understanding the experiences of individuals.

5.6.3 Research Findings

The findings indicate that, beyond the threshold level of trust, societal information privacy concern is low; and trust is high, thereby encouraging further institutional collaboration and acceptance of citizens' informational self-determination.

Trust is what moderates and mediates citizens' privacy concerns and citizens attitudes towards IdMS. Thus, individuals are likely to engage in transactions, if their level of trust exceeds their personal privacy concern threshold, which is reached, when the potential benefits outweigh the risks. This threshold will always depend on the type of transaction and the amount of identifiable information revealed. For instance, transactions requiring the revelation of other attribute data (Wilton, 2008a) might require a lower trust threshold. Figure 35 Privacy concern Trust Model illustrates this point.

Thus, when positive steps (i.e., data minimisation) are taken to improve the IdMS, the moderating effect of trust will cause citizens to revise their attitude towards the IdMS, leading to more trust in the credential issuers and the technology and thereby moving threshold downwards, and to the right on the trust curve. Similarly, any negative actions on the part of credential issuers will increase the privacy concern, thereby causing a move upwards and to the left of the privacy trust curve.

The study also observed the need to move away from an undue focus on credentials towards unique identification. This is due to the fact that credential usually encapsulates attributes and entitlements and thus the tendency to equate such documents as representing the identity of a person when in fact they might not be representing a given context or might reveal more information than necessary.

5.6.4 Contributions

The key contribution of the study is the development of the privacy concern-trust curve which clearly demonstrate the two steps towards establishment of a trusted identity framework. Identity relationships usually begin with a low level of trust and a high level of privacy concerns. Once the the initial problems are identified and addressed, it is possible to pass a threshold level of trust, thereby reducing privacy concerns and paving the way for business and interaction. This is the point at which societal trust in Identity service providers is high enough to encourage institutional collaboration (Shirish C. Srivastava & Teo, 2005; Teo e al., 2008), and citizens' informational self-determination (Deci, Connell, & Ryan, 1989b). We also highlight the need for policy makers to categorise personal information in a way that will encourage secondary uses of personal information whilst ensuring that sensitive personal information is released only to legitimate users.

5.6.5 Limitations

This study focused mainly on citizens' attitudes towards identification systems in Ghana and that poses a number of issues in terms of its generalizability that will need to be tested. For instance, there are peculiar dynamics pertaining to every country and for that matter, the inferences drawn might not be representative for all countries. Moreover, the use of a qualitative research approach also gives room for inferences that are not tested empirically, as is the case of quantitative research. In the future, it will be interesting to examine quantitatively the relationship between trust and privacy concerns in relation to citizens' attitudes towards identity management systems.

5.7 Towards Trusted National Identities Framework

The study is an attempt to integrate some of the previous findings as a means of proposing guidelines for establishing trust in an identity ecosystem. The paper discusses the key concepts of trust, personal information uses and information privacy. A model of trusted identity framework is introduced in this paper.

5.7.1 Research Objective and Methods

The study examined the key requirements for crafting a trusted identities ecosystem by adapting DeLone and McLean information systems (IS) success model (Petter et al., 2008, 2012; Urbach & Müller, 2012). Due to the multi-stakeholder nature of national identity management, the study adopts a research approach that engages the key actors and hence a qualitative methodological approach was deemed the most appropriate means for data collection (Creswell, 2007a; Yin, 2011b). The study is based on results from two stakeholder workshops in Ghana, focus group discussions and a series of interviews.

5.7.2 Research Findings

This paper mainly presented a reconstructed subset of the research themes that were explored during the stakeholder workshop, focus group discussions and the interviews (E. Whitley & Kanellopoulou, 2010a). Participants' accounts of their experiences and impressions clustered around the following key thematic areas: Empowerment, system quality, institutional cooperation, quality of service and information quality. For instance, a lack of user involvement or awareness usually affects the opinions and perceptions of a system (F. D. Davis et al., 1989). Another interesting finding of the study is that for IdMS to be effective, there is the need for institutional cooperation and user empowerment. Moreover, the success must be redefined with respect to IdMS since many of government issued credentials are coercive in nature and thus 'use' might not be a good measure of IdMS success.

5.7.3 Contributions

This study has shown that to ensure trusted identities, each stakeholder must be able to authenticate and verify identities on common terms and understanding. Thus, it is not enough to focus on system quality but also institutional cooperation and interoperability with respect to technology, legal framework and standards on the supply side. On the demand side, there is the need for user empowerment in addition to service and information quality.

The study has also shown that any attempt to ensure institutional cooperation and collaboration have the effect of enriching the trust within the identity ecosystem. In effect, through a collaborative effort and societal empowerment, it is possible to realise trusted identities, which have the effect of pushing the relationship between trust and privacy concern. This is an interesting contribution to IdMS research, and identity policy formulation.

5.7.4 Limitations

The major limitation of the paper lies in the fact that the relationshipship between trust and privacy concern as presented in the privacy concern – trust curve is not tested empirically using quantitative methods.

Chapter 6 Discussions

This chapter re-examines and expound on the findings in Chapter 5 by piecing the major themes together in the light of the research objectives in Chapter 1, context and theoretical framework in Chapters 2 and 3 respectively and the research methodology in Chapter 4. The overarching goal of this exercise is to highlight the key factors that affect the effectiveness of IdMS and to propose guidelines for ensuring trusted identity ecosystem. Exposition of the emerged themes thus helps in focusing on those outcomes from the study which specifically impact on IDMS effectiveness or complement the creation of guidelines for a trusted identity ecosystem.

6.1. Emerging Themes

The findings from the various sources of evidence projects the major factors that affect the IDMS effectiveness, a prerequisite for the trusted identity ecosystem. These include; a strong emphasis on stakeholder involvement, effective civil registration systems, which is an important basis for identity formation and thus a focus on identity and not credentials; system and information quality, service quality and adherence to standards, regulatory and interoperability framework. These emerging themes are depicted in Figure 31. Subsequent sections of this chapter elaborates on the themes and how they impact on IdMS effectiveness or how they contribute to trusted identity ecosystem.

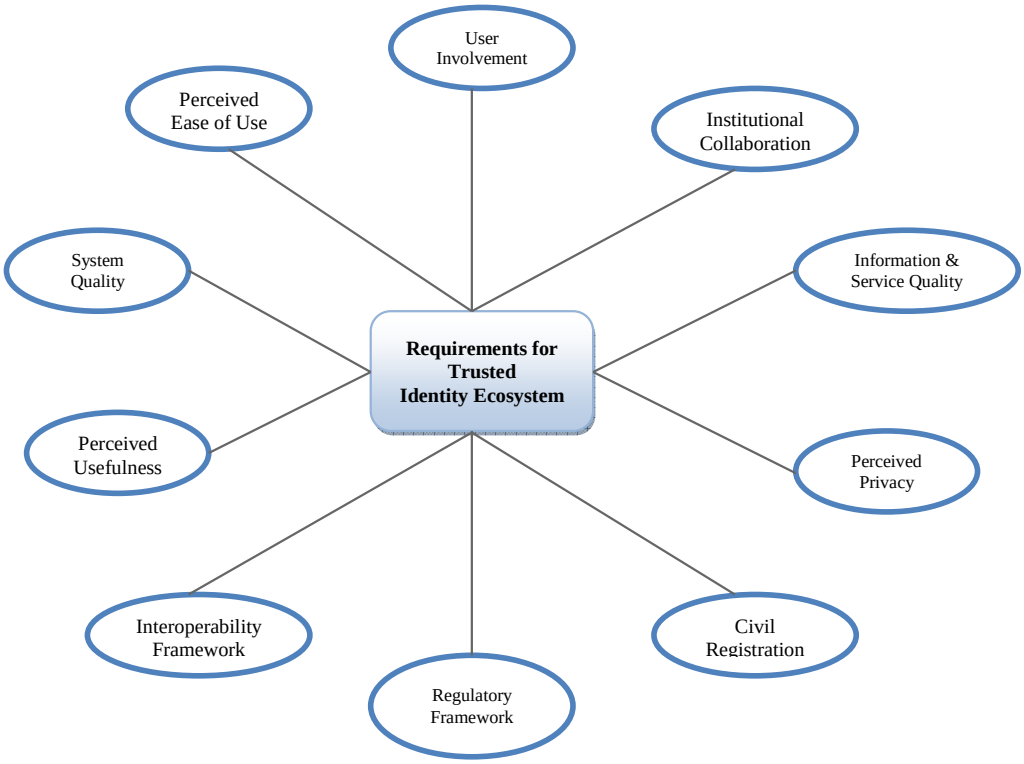


Figure 31 Emerging Themes.

6.1.1. Trusted Identity Framework

These important teams were used to develop the trusted identity framework as depicted in Figure 32. Beyond system quality, information quality, which has been extensively explained in the literature and in Chapter 3, Institutional cooperation, user involvement and empowerment, perceptions on information privacy and trust are the key requirements for a trusted identity ecosystem. This will also ensure that identity can be verified with a high degree of certainty so that business transactions and social interactions could be completed both online and face-to-face with high a degree of confidence.

Figure 32 illustrates the relationships between the major factors that must be observed in defining a trusted identity framework. The figure is an adaptation of the updated DeLone and McLean's IS success model described in Chapter 3. Thus institutional cooperation, system quality and information are key factors that influence trustworthiness. Similarly, user empowerment, and service quality influence perception of privacy, since they have direct impact on user consent and control, minimum disclosure, etc. Thus information quality has a direct impact on both trust and privacy. The moderation and mediation effect of trust can either positively or negatively affect user concerns depending on the level of trust as illustrated in Figure 35.

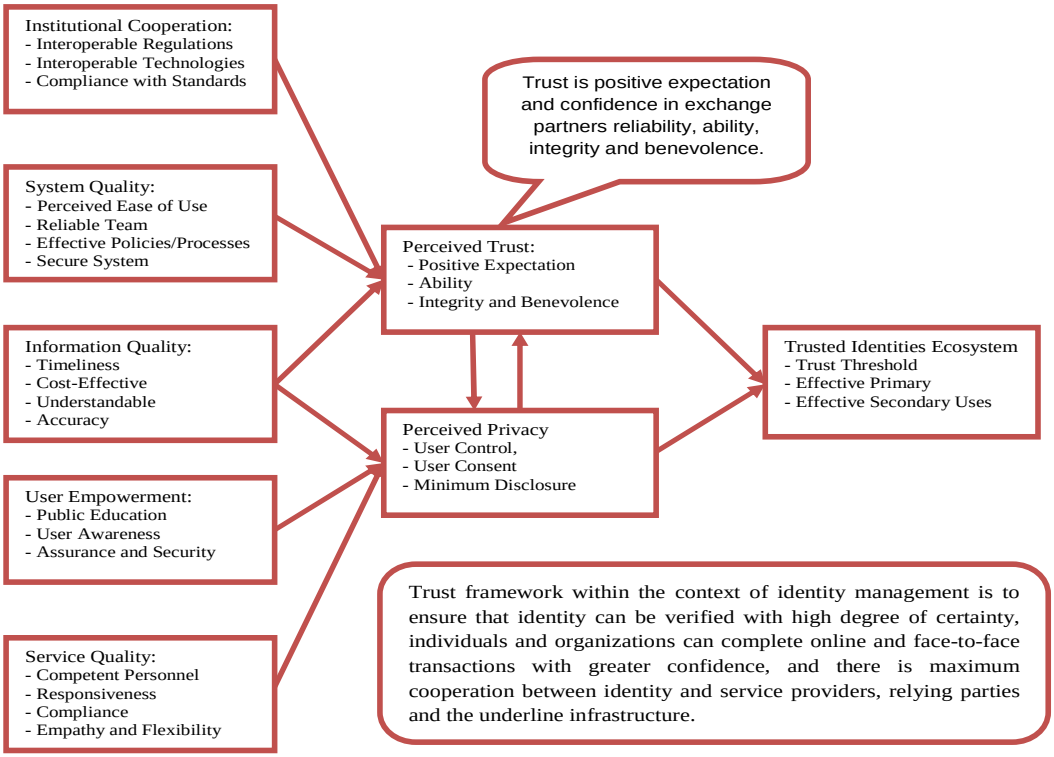


Figure 32 Trusted Identities Framework.

6.1.2 Stakeholder involvement

The absence of stakeholder involvement in identity policy formulation leads to a certain lack of trust in institutions. Key stakeholder participation in identity policy formulation could be very instrumental in courting users‘ trust and the effectiveness of the identity policy. Such user involvements also provide a means for users to provide important feedback on certain decisions and actions of the identity providers by enabling transfer of trust amongst them (Pavlou & Gefen, 2004). The remarks of a focus group participants and respondents in an interview do highlight the importance of such involvement:

“I feel that I have contributed to the identity policy, If my suggestions are implemented. Unfortunately, what they tell us at the beginning is usually different from what the identity providers give to citizens. For instance, during the voter registration, we thought we were going to receive an innovative voter ID cards but we ended up receiving a laminated card which can easily be copied”. “We were told by the EC that a biometric voting system is being introduced, in the end, the head of the EC said the voting system remains manual and biometric verification was only to complement the manual system”. “Even if I have any feedback, i do not know how to inform them”.

In view of such remarks, there is the need for the utilisation of effective channels of taking constructive and positive feedback. By informing key stakeholders about their actions, identity providers can reinforce citizens’ trust in such institutions. A possible means of getting user involvement is a dedicated feedback unit or Web site to track and respond to identity related concerns and to inform citizens of latest developments. This scheme could be very instrumental in engendering citizens’ trust identity and service providers.

Generally, citizens might perceive identity policies as complex, confusing and too technical and thus additional considerations includes:

- Greater transparency in the enrolment processes and the transfer processes for identity data are key issues to enabling them to make informed choices.
- Public education and awareness programs can help consumers and citizens manage their digital identities appropriately.
- Defining accountability and transparency measures across multiple services in diverse legal and technical regimes is an important issue in user empowerment.

6.1.3 Interoperability

A major issue that emerged from the finding of papers 3 is the requirement for interoperable IDMS policies and standards. This was noted during the two workshops, focus group discus-

sions and interview responses. The following remarks typified such frustration; *"Why can't I present my drivers' license as proof of identity for voting in an election, if I misplace my voter ID card; and why can't I present my voter ID as proof of my qualification to drive, if the police stops me whilst driving*?. *In any case, all these documents bear my name and other details and I have not travelled outside the country"*.

The policy, legal, business process and technical implication of an interoperability framework includes:

- Policy level: The challenge for organisations will be for each key actor being able to articulate a clear set of IdM policies containing a common set of elements which highlight areas of compatibility and disparity.
- Legal level: Compatible internal and international regulations and compliance obligations across organisations will facilitate legal interoperability. The legal issues also include the need to address major contractual obligations.
- Technical level: The challenge is to encourage the development and use of all types of standards, in the broadest senses, without stifling competition or undermining innovation.
- Business process level: Issues also arise at the business process level, where progress towards the adoption by organisations of common methods for IdMS to communicate with each other may need to be considered.

In many developing countries, the interoperability policies have been formulated and what is necessary is their enforcement.

6.1.4. Ensuring Privacy

The information in an IdMS is mainly comprises of personal information and thus any lapses or insufficient privacy and data security controls in the use of the system could lead to adverse consequences for data subjects, whereas effective deployment of the IdMS could play a privacy protective role, particularly in the context of social interactions. It is therefore imperative that privacy considerations are made with respect to data collection, data usage and storage, data minimisation, anonymity, pseudonymity. Moreover, users must be aware of the extent to which they can exercise control over how their personal data is used and how to exercise such controls. Some of the important information privacy issues include:

- The potentially unlimited lifespan of digital identity information and the declining costs of storage and processing raise issues regarding long-term assurances of safe storage and appropriate usage, and highlight the value of eliminating identity-related personal information when it is no longer needed.

- There is a risk that the greater availability of credentials from high-level assurance systems could increase their use in systems with lower-level assurance needs. This could increase the risk to personal data.
- Linking identities that do not share the same degree of anonymity, or that contain different sets of attributes may allow others to overcome pseudonyms and discover the user's identity.
- Differences may arise as to which practices of identity and other data collection, use, and retention can be left to market forces and those that should be the subject of government intervention.

To address such issues, it is important to implement identity policies that facilitate anonymity and pseudonymity depending on the context. Clear policies must also be implemented to address issues regarding who has the right to decide which data should be disclosed and the circumstances under which it might be encrypted. This is particularly important to the exercise of informational self-determination.

6.1.5 Trust in Institutions

Trust in institutions emerged as a vital element for adoption and usage of any government initiatives since it is based on cognitive processes that tend to discriminate trustworthy institutions from others (J. D. Lewis & Weigert, 1985). A remark by one of the respondents below reflects the general feelings of citizens:

"If the systems were to be run by qualified personnel, identity abuses like forged passports and driving licenses will be minimised. The appointment of many of the key decision makers in these organizations is based on factors other than qualification and experience. We only use it because we have no option for an alternative".

Such statements clearly show a lack of trust in the institutions which issue credentials due to the perception that personnel handling the credentials are unqualified and inefficient. Trust in the institutions is also dependent on citizens' previous experiences with policy enforcement as recounted by another respondent;

"My brother sent me to withdraw foreign currency remittance from abroad, when I got to the bank the following day, I was told I had already collected the money. When I insisted that I had not been to the bank, I was shown a voter identity card bearing my name except the picture was different. I was advised to go to the electoral commission for redress instead. It turned out that the other card was forged and the bank had no means of verifying. So at the

moment I do not trust the voter's ID card or any other credential for that matter since they can easily be forged".

This obviously implies a lack of confidence in identity service providers. Citizens trusting behavior in the identity and service providers usually stems from previous experiences, knowledge and exchanges. Such interactions give citizens the opportunity to access the competences, benevolence, and integrity of identity providers which are the key measures of trustworthiness (R. C. Mayer et al., 1995). These points are clearly illustrated in a citizen's account ot his experiences at the premises of one of the credential issuers;

> *..... I was scared when I read about the number of national identity cards abandoned in the National Identification Authority (NIA) office, because, mine was part of the million cards in the office. My inability to collect my card wasn't because I didn't want it, but because of the hassles one has to go through to obtain his/her card. Monday 3rd September, 2012 was my third visit to the office. In the previous two occasions, I left because I could not wait to follow the queue after an hour. As a staff of an international organization, one is not allowed to stay for such long hours doing personal business. Today's story was different because it was only 20 persons eagerly waiting for their cards no matter what happens. Unfortunately the problem today was because the lights in the building went off. In the collection room were NIA staff who have been responding to angry Ghanaians like myself as if they are glad the lights are off (and hence will have a holiday.....*

Figure 33 My Experience at NIA Office: Source http://vibeghana.com/2012/09/03/.

Where identity providers demonstrate technical knowledge and ability in successful implementation of IdMS, it increases the level of citizen's trust (S. C. Srivastava & Teo, 2009). Similarly, trust increases, if citizens have positive perception of identity providers' ability, intergrity and benevolence by acting in honesty and in the interest of the citizens. Thus so long as perceived government manipulation, and abuse of authority persist, lack of citizens' trust in identity providers will continue. In the above encounter, the ending of the stody shows a frustrated citizens in shown below;

..... I don't have MUCH problem if the issue is just because of crowd, but if it is as a result of lights off, then it's "NOT-NOT-NOT". What if there were people in the lift in the building? Why do we have to let the system go off and takes about 25min to restart. Do we want to frustrate people in the process of collecting their identity cards and at the expense of their job? I like their building and I believe a lot of money went into it. In the same manner, people should be responsible for every gadget in the building for it to function well. In public structures like this, I cannot accept an excuse that there is lights off and accuse ECG. If the Authority want people to come for the cards, then they have to check their current system and make it more functional.....

Source: http://vibeghana.com/2012/09/03/.

Thus, identity providers must take steps to shed away such negative perceptions. For instance, the introduction of biometric voter identity verification system in the 2012 election Ghana resulted in two days of voting and several accusations of system manipulation. Such incidences have the propensity to diminish the trust that citizens have in the identity provider.

6.1.6 Focus on Identity and not Credentials

The processes of citizens identity formation and how individuals are enrolled into identity policies affect the effective of the resulting identity management systems. Thus, where there are weakness in the identity formation and enrolment processes, the reliability of the resulting source documents (i.e. birth certificates) and the issued credentials and the IDMS become questionable. This is reflected in a concern shared by a workshop participant during a question and answer session;

> *"Many of people are not issued with birth certificates at birth and even for those who the information might not be in a reliable database. Individuals have to apply for such documents when they are already old or when it suits them resulting in the use of wrong or incurroct location and data-of-births. "If I am in doubt of the validity of the source document or can't verify its authenticity, why will I trust the agencies to operate in my interest?".*

A common misunderstanding on the part of credential issuers and policy makers which became apparent during the workshop was the equation of strong credentials to effective IdMS. Thus more resources are invested in the technology and not how to ensure the reliability of the information and to make it available to citizens. The following statements coming from credential issuers were common during the workshop and focus group *"we have introduced biometric based ID cards that are difficult to forge"*.

A distinct feature of a credential is that it encapsulates attributes and entitlements in a reliably verifiable form. There is therefore the tendency to equate such documents as representing the identity of a person when in fact they might not be represented in a given context. For instance, passports and driving licenses have historically been presented as foolproof documents loaded with the necessary information that can enable the holder to access services and for authentication purposes. This is not without drawbacks, since it is susceptible to revealing more information about the holder than is necessary in any given authentication context. Using a passport for proof of age will no doubt reveal the passport holder's name, place of birth and citizenship, and a driver's license used for similar purpose can also reveal your date of birth and address.

There is, therefore, the need to move away from credentials towards unique identification. **Error! Reference source not found.** provide a framework for addressing such concern using the model of identity which categorises personal information into three interrelated dimensions. A credential such as a passport or driving license typically includes some attributes in each of the three aspects of identity – the basic idenitifier set (BIS), personally identifiable information (PII) such as height, eye colour; and any sector-specific data such as entitlement to drive specific classes of vehicle, or visas indicating entitlement to enter a specific country.

A focus on identity will also make it easier to enforce policies appropriate to the data in question, particularly when different sector-specific data items entail different policy controls. For instance, entitlement to drive a vehicle may not be part of major privacy concern, whereas credit status will, hence data security policies could be segregated to address such data. On the other hand, since healthcare history and medical conditions are very sensitive, a different set of policies must apply, segregating identity data into sector-specific segments in order to cater for discrete management policies by sector and data type. Thus, within a given data segment, assertions of identity ('the holder of this credential is XX') may make one kind of data security policy appropriate, while assertions of other attributes may require quite different policy treatment.

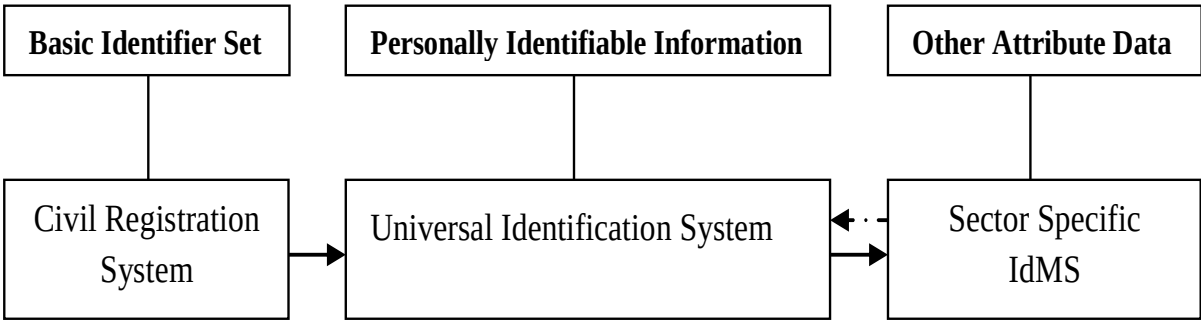


Figure 34 A Model of Identity.

6.2 Requirements for Trusted Identity Ecosystem

Trust is what moderates and mediates citizens' privacy concerns and attitudes towards IdMS. Thus, individuals are likely to engage in transactions, if their level of trust exceeds their personal privacy concern threshold, which is reached, when the potential benefits outweigh the risks. This threshold will always depend on the type of transaction and the amount of identifiable information revealed. For instance, transactions requiring the revelation of other attribute data (**Error! Reference source not found.**) might require a lower trust threshold.

Thus, when positive steps (i.e., data minimisation) are taken to improve the IdMS, the moderating effect of trust will cause citizens to revise their attitude towards the IdMS, leading to more trust in the credential issuers and the technology and thereby moving down and to the right on the trust threshold.

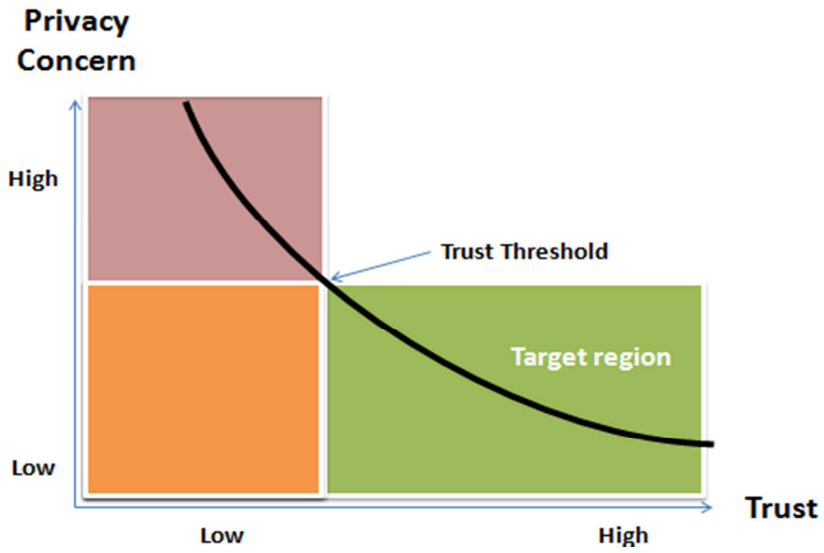


Figure 35 Privacy concern Trust Model.

Similarly, any negative actions on the part of credential issuers will result in a diminishing level of trust, thus, increasing citizens' concern and thereby causing a move upwards and to the left of the privacy-concern-trust curve. The trusted identity framework in the United States, where the interest of all stakeholders in the identity ecosystems is taken into account, is a clear step taken by the US government to increase trust (Bertino, 2012; Grant, 2011b).

Trusted identity ecosystems also depend on the availability of choice to citizens. In a recent European survey; a*round two-thirds of Europeans use credit cards and bank cards. When respondents were asked which type* credentials they use, 74% of respondents use credit cards and bank cards (74%), and about two-thirds use national identity cards or residence permits (68%), government entitlement cards (65%), or driving license (63%). This is a clear indica-

tion of user confidence in financial institutions as shown in Figure 36 below. It also shows the diminishing importance of certain credentials in a day to day transaction.

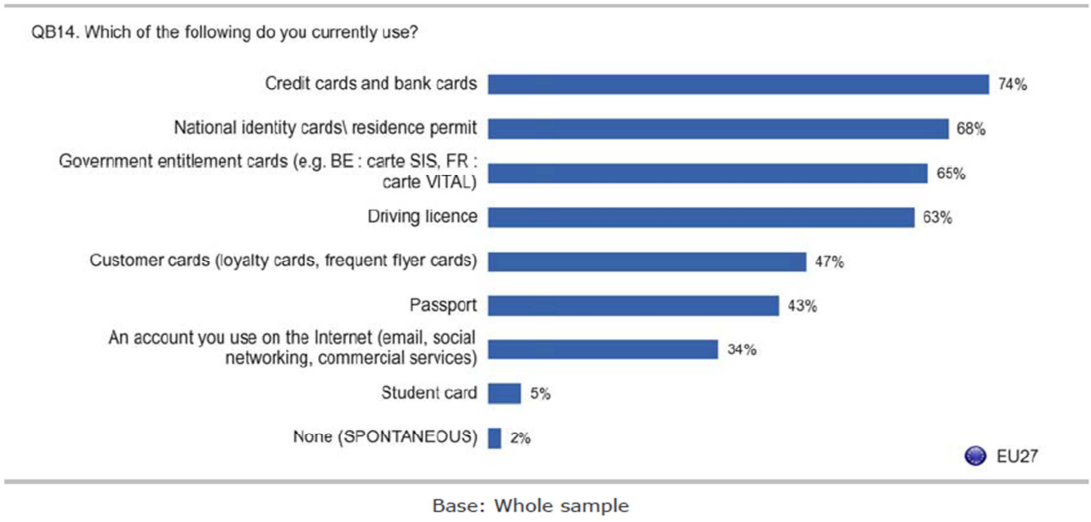


Figure 36 Major Credentials Used in the European Union (TNS Opinion & Social, 2011).

Chapter 7 Conclusion and Further Studies

This research was conducted in a space of three years . In this period of time, I have engaged in a number of discourses with industry practitioners as well as academicians and I have also read a substantial body of literature. Trusted identity framework and privacy-concern-trust curve are products of all these interactions.

While I have worked towards contributing to theory and practice, I also acknowledge the fact that attempting to encompass all the issues and all the relationships in the domain of identity management will be a project in futility. Thus, as posited by Feyerabend (1993:39) "we may start by pointing out that no single theory ever agrees with all the known facts in its domain. Therefore I do not suggest that my findings are the only answers to the research questions that I set out to answer, since there could be alternative views upon which trusted IDMS is based. Similarly, there could be other contextual factors that I might have ignored which is a matter of further research to develop, extend or disprove the claims presented in this thesis. Hence, within the context of reliability of the research approach, verifying and confirming the research outcomes, I can conclude that what I have presented are the competent and useful answers to the research questions at this point in time.

The concepts of identity and digital identity are central to contemporary business transactions and social interactions. The criticality of such a phenomenon emanates from identity service providers' utilitarian attitude towards issues of security, privacy and trust. Thus, IDMS developers and identity service providers especially those in developing countries have the tendency of addressing privacy and trust issues from the perspectives of ease, personal data collection and usage, whilst dealing with information privacy the same way official secrecy is treated. The result therefore is the equation of secrecy to privacy although identity issues transcend data collection and storage.

Identity policy makers and IdMS developers must therefore take steps back from focusing on credentials towards identity itself and the underlying relationships that are present in the identity eco-system. Thus, the need to also consider the context within which the IdMS and identity policies are implemented, and to analyse the impact of identity policies on the lived experiences of data subjects (Rahaman & Sasse, 2010).

This dissertation has charted both historical and phenomenological paths to research and addresses such requirements in the formation of trust in identity policies regarding identity formation and identity management systems. It also highlights the factors needed to be taken into consideration in meeting the trust threshold.

A multi-method qualitative research approach was employed to understand these factors. The insights from the research are in this concluding section captured as crafting a trusted citizen-centered identity policy.

7.1 Crafting a Trusted Identity Policy

The research questions 1, 2 and 3 sought answers about the major factors that contribute to trusted IDMS that is privacy enhancing. The research findings suggested that contrary to the assumptions that perceived usefulness and perceived ease of use are the major determinants to IS effectiveness, rather it is the perceptions of trust and privacy that form the major determinants. Thus, user empowerment and institutional collaborations were major determinants of the effectiveness of such systems. The proposal for user empowerment is also grounded in OECD privacy guidelines regarding user control and consent principles, thus implying its significance to the effective uses of IDMS. User experiences and exposure to technologies (especially the Internet, credit card uses) and cues in social surroundings minimises the risk of abuses of personal identity information.

The solutions to the research questions thus underscore the need for a critical analysis of the artifact and context of the study (Orlikowski & Iacono, 2001). In other words, the specificities of artifacts and the process of their shaping need to be reflected in our conceptualizations and in the theoretical and methodological apparatus applied to generate theory. This is very important in ideas and answers to key issues which had hitherto stymied effective uses of IDMS.

The study has also opened an array of channels which allow the flow of future research on trusted identity management systems. The privacy concern trust model and the trusted identiy framework are novel ideas that give policy makers a better understanding of steps that must be taken to ensure effective uses of IDMS. Despite the numerous research initiatives on identity management in general and user centricity in particular, the concepts of trust and privacy remain a dilemma, not just for users and service providers but for all stakeholders in the identity ecosystem. It seems there is a continued surge in proposed solutions that coarsely address user requirements and then leaving out the fine-grained aspects of identity management which is what will trigger an effective identity ecosystem.

Addressing such fine-grain issues required a multi-stakeholder approach using qualitative research methods to research which is what this study sought to achieve. This is not withstanding the fact that the study could have equally been approached objectively using quantitative research approach. However, such an approach would have ignored certain tacit information that can only be extracted from the minds of people who are engaged in conversation.

Thus, such complexities in a phenomenon having multi-actor perspective required the involvement of the key actors in the decision making process and the analysis of the phenomena in the context (Lee, 2001).

It is my hope that this pursuit as outlined in the thesis and culminating in the development of the privacy concern trust framework contributes to extending human understanding of the phenomena.

Another important strength of this research lies in the application of stakeholder approach and the adaptation of D&M IS success model to examine IS effectiveness and bringing OECD countries' perspectives to bear on identity policies in developing countries. The study also highlights key aspects of identity policies that seem to be disregarded in IDMS research.

Thus the study has offered a means of communicating key design principles and guidelines to IdMS developers and policy makers using diverse data collection and analysis, in an attempt to demonstrate how such issues associated with personal information are not to be taken for granted. The findings from the study highlights the urgency that is required to be applied in indentity policies. Interesting developing countries stand to lose the most if such remedial actions are not taken to avert the fundamental issues in identity policies which have culminated to the fragmented nature of IdMS. For instance the year 2012 biometric based voter registration exercise in Ghana cost $82,326,497.00 as compared to $12,437,000.00 in the year 2004, indicating an astronomical percentage increase of about 562%. In contrast to a country like Denmark, where there is a relatively reliable civil registration system, such expenditure is avoidable, since the electoral register is usually generated from the CRS. Ironically, the high enrolment cost in Ghana has also not improved trust in the system as it is exemplified in the outcome of 2012 presidential elections in which for the first time in the country's history, the validity of the results declared is being challenged at the supreme court be some of the key stakeholders.

The adaptation of the IS success model to the phenomenon of the trusted identity management system, in addition to adding to existing sequence of IS literature, has also brought to the fore, context specific issues in developing countries to understand their extent of influence especially in a substitution instead of complementary environment.

During the workshops and focus group discussion, a discovery was made to the fact that users appreciate the benefits of legitimate secondary uses of personal information and rather, the challenge to effective uses of personal information arises from policy makers and identity providers' attitude to such information, by treating the privacy as part of official secrecy.

It seems to me that researchers and developers implicitly assume that sometimes all users have attained a certain level of literacy and exposure to appreciate the supposed patch-work meant to plug the gaping gap created by the lack of an identity layer on the Internet. Such a presumption is seen in many of the prescriptions such as the laws of identity (Kim Cameron, 2005), and OECD privacy guidelines (OECD, 2011a). Such attitudes if not checked will continue to discredit the relevance of the resulting technologies in developing countries, although the alarming growth in digital IdM technology in these sub-regions provide a great market potential.

Another interesting aspect of this study is the advocating of a move away from undue focus on physical verification of credentials towards Internet and mobile applications using identity data for authentication purposes. This move will open up several opportunities for application developers to develop cutting-edge solutions for businesses since successful secondary uses of personal information have the tendency to improve trust in the identity ecosystem.

Finally, the mechanisms of establishing trust in the physical world are not necessarily the same as those that are used in the digital world online. However, since physical identity credentials are used in both worlds, there is the need for more work on linking usage in order to achieve more human integration. It is thus concluded that researchers should develop identity management systems that ensure that users can feel comfortable consuming services in the physical and digital worlds (J. K. Adjei & Olesen, 2011). Thus individuals seek to assert not their physical being as such, but rather an informational representation of the chain of life events that is defined by who they are.

7.2 Implications for Practitioners and Scholars

BCG estimates that two-thirds of the potential digital identity value – or about €440 billion in 2020 alone , is at risk if stakeholders fail to establish a trusted flow of personal data. Identity policy makers, identity providers, service providers, identity and security technology driven organizations represent the audience who stands in good stead to benefit from the findings and contributions of this study. Thus it should remind identity policy makers and identity providers that for a national IDMS to be effective, measures must be taken to ensure the attainment of at least, the trust threshold. The minimum level of trust required for institutional collaboration, IDMS interoperability, user involvement and legitimate secondary uses and commercialisation of personal information.

Also, designers and policy makers must take context specific issues into consideration and thus, offer citizens' IdMS that address their basic transactional and interaction needs which is

their day-to-day “lived” experiences and social practices (Rahaman & Sasse, 2010). More specifically, it is observed that countries with strong civil registration systems in the long run benefit more from identity policies and comparatively spend less in addressing identity issues in interpersonal communication.

7.3 Further Studies and Limitations

Research in this area could be advanced by looking at developing a model for mapping institutions’ trust threshold levels. Such a study will be very useful in finding out a particular organisation’s trust threshold and the measurement of institutional progress with respect to trust that users have in them and the IdMS. A key proposal in this study is the need to strengthen the civil registration system as a key measure in ensuring effective and trusted identity ecosystem. A study that evaluates the impact of CRS post implementation on trusted identity ecosystem will also be a very interesting contribution to citizen centric IDMS research and practice.

Further analysis of the demographic major factors and in the use of IdMS may increase our understanding of the policies required to cater for such specifics. For example, how does the privacy practices of women differ from men and how does the privacy practices of adult differ from the youth. This exercise is not static and as such my future endeavour will be, an attempt to address such requirements using the rich data and insight acquired during the study.

References

3G_Americas. (2009). *Identity Management; Overview of Standards & Technologies for Mobile and Fixed Internet*. Retrieved from http://www.4gamericas.org

Abelson, H., & Lessig, L. (1998, December 10). Digitial Identity in Cyberspace. Retrieved December 24, 2012, from http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall98-papers/identity/white-paper.html

Adjei, J. K. (2012, November 7). Ghana needs to strengthen civil registration system. *Ghanaweb*. Retrieved December 18, 2012, from http://www.ghanaweb.com/GhanaHomePage/regional/artikel.php?ID=255638&nav=next

Adjei, J. K., & Olesen, H. (2011). Analysis of Privacy-Enhancing Identity Management Systems. Presented at the WWRF Meeting #26, Doha, Qatar. Retrieved from http://vbn.aau.dk/ws/files/61836738/WWRF_2011_Analysis_of_Privacy_Enhancing_IDMS_final_.pdf

Adjei, J. K., & Olesen, H. (2012). Building Trusted National Identity Management Systems. In CENTRIC 2012, The Fifth International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services (pp. 19–26).

Adjei, J., & Olesen, H. (2011). Keeping Identity Private. *IEEE Vehicular Technology Magazine*, *6*(3), 70–79. doi:10.1109/MVT.2011.941894

Afari Gyan. (2012, December 11). Election results reflect the people's true will – Afari Gyan. *citifmonline.com*. Retrieved January 14, 2013, from http://citifmonline.com/?id=1.1182548

Aichholzer, G., & Strauß, S. (2009). The Citizen's Role in National Electronic Identity Management - A Case-study on Austria. In *Second International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2009. CENTRIC '09* (pp. 45 –50). doi:10.1109/CENTRIC.2009.13

Aichholzer, Georg, & Strauß, S. (2009). Understanding a complex innovation process: identity management in Austrian e-government. In *Proceedings of the 10th Annual International Conference on Digital Government Research: Social Networks: Making Connections between Citizens, Data and Government* (pp. 230–239). Digital Government Society of North America. Retrieved from http://dl.acm.org/citation.cfm?id=1556176.1556218

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, *50*(2), 179–211.

Ajzen, I., & Fishbein, M. (1977). Attitude-behavior relations: A theoretical analysis and review of empirical research. *Psychological Bulletin; Psychological Bulletin*, *84*(5), 888.

Alatalo, T., & Siponen, M. T. (2001). Addressing the personalization paradox in the development of electronic commerce systems. In *Post-proceedings of the EBusiness. Research Forum (eBRF), Tampere, Finland*. Retrieved from http://owla.oulu.fi/publications/ebrf-personalisation.pdf

Almutairi, H., & Subramanian, G. H. (2005). An empirical application of the DeLone and McLean model in the Kuwaiti private sector. *Journal of Computer Information Systems*, *45*(3), 113–122.

Almutairi, Helail, & Subramanian, G. H. (2005). An Empirical Application of the DeLone and Mclean Model in the Kuwaiti Private Sector. *Journal of Computer Information Systems*, *45*(3), 113–122.

Alsabawy, A. Y., Cater-Steel, A., & Soar, J. (2012). A model to measure e-learning systems success. Retrieved from http://eprints.usq.edu.au/20715

Andrade, E., Kaltcheva, V., & Weitz, B. (2002). Self-disclosure on the Web: the impact of privacy policy, reward, and company reputation. *Advances in Consumer Research*, (29), 350–353.

Armando, A., Carbone, R., Compagna, L., Cuéllar, J., Pellegrino, G., & Sorniotti, A. (2012). An authentication flaw in browser-based Single Sign-On protocols: Impact and remediations. *Computers & Security*, (0). doi:10.1016/j.cose.2012.08.007

Aveyard, H. (2010). Doing a literature review in health and social care. Open University Press.

Baldwin, A., Casassa Mont, M., Beres, Y., & Shiu, S. (2010). Assurance for federated identity management. *Journal of Computer Security*, *18*(4), 541–572. doi:10.3233/JCS-2009-0380

Bannister, F., & Connolly, R. (2011a). Trust and transformational government: A proposed framework for research. *Government Information Quarterly*, *28*(2), 137–147.

Bannister, F., & Connolly, R. (2011b). The Trouble with Transparency: A Critical Review of Openness in e-Government. *Policy & Internet*, *3*(1), 158–187.

Barki, H., & Hartwick, J. (1989). Rethinking the concept of user involvement. *MIS quarterly*, *13*(1), 53–63.

Barki, Henri, & Hartwick, J. (1994). Measuring User Participation, User Involvement, and User Attitude. *MIS Quarterly*, *18*(1), 59–82. doi:10.2307/249610

Becker, H. S. (1970). Field work evidence. *Sociological work: Method and substance*, 39–62.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017–1042.

Bélanger, France, & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS Q.*, *35*(4), 1017–1042.

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly*, *11*(3), 369–386. doi:10.2307/248684

Bennett, C. J., & Raab, C. D. (2003a). *The governance of privacy : policy instruments in global perspective*. Aldershot; Burlington, VT: Ashgate.

Bennett, C. J., & Raab, C. D. (2003b). *The governance of privacy : policy instruments in global perspective*. Aldershot; Burlington, VT: Ashgate.

Bertino, E. (2012). Trusted Identities in Cyberspace. *IEEE Internet Computing*, *16*(1), 3 –6. doi:10.1109/MIC.2012.15

Bertino, E., Paci, F., Ferrini, R., & Shang, N. (2009). Privacy-preserving digital identity management for cloud computing. *Data Engineering*, *32*(1). Retrieved from ftp://ftp.research.microsoft.com/pub../debull/A09mar/bertino.pdf

Bertino, E., & Takahashi, K. (2010). *Identity Management: Concepts, Technologies, and Systems*. Artech House Publishers. Retrieved from http://books.google.co.uk/books?hl=en&lr=&id=UrmD-Gxt-

8IC&oi=fnd&pg=PA5&dq=Identity+Management+Concepts,+Technologies,+and+Systems&ots=jlQzxC--kR&sig=dBMXV8CA9G3aHi2IdugvstliKe0

Bhalla, J. (2012, November 17). Can tech revolutionize African elections? *CNN*. Retrieved December 30, 2012, from http://www.cnn.com/2012/11/17/opinion/sierra-leone-election-biometric/index.html

Bird, A. (2012). The Structure of Scientific Revolutions and its Significance: An Essay Review of the Fiftieth Anniversary Edition. *The British Journal for the Philosophy of Science*, *63*(4), 859–883. doi:10.1093/bjps/axs031

Biskup, J., & Brüggeman, H. H. (1988). The personal model of data:: Towards a privacy-oriented information system. *Computers & Security*, *7*(6), 575–597.

Blume, P. (1989). The personal identity number in Danish law. *Computer Law & Security Review*, *5*(3), 10–13. doi:10.1016/0267-3649(89)90030-7

Boland, R. J., & Day, W. F. (1989). The experience of system design: a hermeneutic of organizational action. *Scandinavian Journal of Management*, *5*(2), 87–104.

Bourdieu, P. (1996). Understanding. *Theory, Culture & Society*, *13*(2), 17–37. doi:10.1177/026327696013002002

Bratton, M. (1998). Second elections in Africa. *Journal of Democracy*, *9*(3), 51–66.

Bryman, A. (2012). *Social Research Methods*. Oxford University Press.

Bulmer, M. (2011). Concepts in the analysis of qualitative data. *The Sociological Review*, *27*(4), 651–677.

Burton-Jones, A., & Straub, D. W. (2006). Reconceptualizing System Usage: An Approach and Empirical Test. *Information Systems Research*, *17*(3), 228–246. doi:10.1287/isre.1060.0096

Camenisch, J. (2012). Information Privacy⁈. *Computer Networks*. Retrieved from http://www.sciencedirect.com/science/article/pii/S1389128612003660

Camenisch, J., Krontiris, I., Lehmann, A., Neven, G., Paquin, C., Rannenberg, K., & Zwingelberg, H. (2011). *D2. 1 Architecture for Attribute-based Credential Technologies–Version*. Technical report, ABC4Trust Consortium (December 2011), https://abc4trust. eu/index. php/pub/107-d21architecturev1. Retrieved from https://abc4trust.eu/download/ABC4Trust-D2.1-Architecture-V1.pdf

Cameron, K., & Jones, M. B. (2007). Design rationale behind the identity metasystem architecture. *ISSE/SECURE*, 117–129.

Cameron, Kim. (2005, May). The Laws of Identity. Retrieved December 26, 2012, from http://msdn.microsoft.com/en-us/library/ms996456.aspx

Cameron, Kim. (2010, July 3). IdentityBlog - Digital Identity, Privacy, and the Internet's Missing Identity Layer. Retrieved May 13, 2013, from http://www.identityblog.com/?p=1142

Cavalier, R. (2003). *Plato for beginners*. Orient Blackswan.

Cavaye, A. L. M. (1995). User participation in system development revisited. *Information & Management*, *28*(5), 311–323.

Cavaye, A. L. M. (2008). Case study research: a multi-faceted research approach for IS. *Information systems journal*, *6*(3), 227–242.

Cavoukian, A. (2012). Privacy by design. *Report of the Information & Privacy Commissioner Ontario, Canada*. Retrieved from

http://privacybydesign.ca/content/uploads/2012/04/Privacy-by-Design-Origins-Meaning-and-Prospects.pdf

Cavoukian, A., & Carter, F. (2006). *7 laws of identity: The case for privacy-embedded laws of identity in the digital age*. Information and Privacy Commissioner of Ontario.

Chan, C. M. L., & Pan, S. L. (2008). User engagement in e-government systems implementation: A comparative case study of two Singaporean e-government initiatives. *The Journal of Strategic Information Systems*, *17*(2), 124–139.

Chen, W. S., & Hirschheim, R. (2004). A paradigmatic and methodological examination of information systems research from 1991 to 2001. *Information Systems Journal*, *14*(3), 197–235.

Cheng, Y. (2012). Case Studies of Success Model of Gas Industry Underground Pipeline Information System. Retrieved from http://pc01.lib.ntust.edu.tw/ETD-db/ETD-search/view_etd?URN=etd-0625112-191638

Clarke, R. (1994). Human identification in information systems: Management challenges and public policy issues. *Information Technology & People*, *7*(4), 6–37.

Clarke, R. (1999). Introduction to dataveillance and information privacy, and definitions of terms. *Roger Clarke's Dataveillance and Information Privacy Pages*. Retrieved from http://www.cse.unsw.edu.au/~cs4920/seminars/resources/Roger-Clarke-Intro.pdf

Clarke, Roger. (1994). The digital persona and its application to data surveillance. *The Information Society*, *10*(2), 77–92. doi:10.1080/01972243.1994.9960160

Clarke, Roger. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, *42*(2), 60–67. doi:10.1145/293411.293475

Clarkson, M., & others. (1998). The corporation and its stakeholders: classic and contemporary readings. University of Toronto Press.

Cofta, P. (2008). Towards a better citizen identification system. *Identity in the Information Society*, *1*(1), 39–53.

Connolly, P. J. (2010). OAuth is the'hottest thing'in identity management. *eWeek*, *27*(9), 12–13.

Connolly, R., Bannister, F., & Kearney, A. (2010). Government website service quality: a study of the Irish revenue online service. *European Journal of Information Systems*, *19*(6), 649–667.

Crane, A., & Ruebottom, T. (2012). Stakeholder Theory and Social Identity: Rethinking Stakeholder Identification. *Journal of Business Ethics*, *102*(S1), 77–87. doi:10.1007/s10551-011-1191-4

Creswell, J. W. (2007a). Qualitative inquiry and research design : choosing among five traditions. Thousand Oaks: Sage Publications.

Creswell, J. W. (2007b). Qualitative inquiry and research design : choosing among five traditions. Thousand Oaks: Sage Publications.

Crompton, M. (2004). Proof of ID Required? Getting Identity Management Right. Australian IT Security Forum.

Crosby, J. (2008a). Challenges and opportunities in identity assurance. London: HM Treasury].

Crotty, M. (1998). The foundations of social research: Meaning and perspective in the research process. Sage Publications Limited.

Culnan, M. (1993). “How Did They Get My Name?” An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use. *Management Information Systems Quarterly*, *17*(3), 341–363.

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, *10*(1), 104–115. doi:10.1287/orsc.10.1.104

Daase, C., & Kessler, O. (2007). Knowns and Unknowns in the `War on Terror’: Uncertainty and the Political Construction of Danger. *Security Dialogue*, *38*(4), 411–434. doi:10.1177/0967010607084994

Dass, R., & Pal, S. (2009). *Feasibility and Sustainability Model for Identity Managament*. Indian Institute of Management. Retrieved from http://www.iimahd.ernet.in/publications/data/2009-12-01Dass.pdf

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13*(3), 319–340. doi:10.2307/249008

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management science*, *35*(8), 982–1003.

Davis, Fred D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q.*, *13*(3), 319–340. doi:10.2307/249008

De Villiers, M. R. (2005). Three approaches as pillars for interpretive information systems research: development research, action research and grounded theory. In *Proceedings of the 2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries* (pp. 142–151). Republic of South Africa: South African Institute for Computer Scientists and Information Technologists. Retrieved from http://dl.acm.org/citation.cfm?id=1145675.1145691

Deci, E. L., Connell, J. P., & Ryan, R. M. (1989a). Self-determination in a work organization. *Journal of Applied Psychology*, *74*(4), 580–590. doi:10.1037/0021-9010.74.4.580

Deci, E. L., Connell, J. P., & Ryan, R. M. (1989b). Self-determination in a work organization. *Journal of Applied Psychology*, *74*(4), 580–590. doi:10.1037/0021-9010.74.4.580

Delone, W. H., & McLean, E. R. (2003). The DeLone and McLean Model of Information Systems Success: A Ten-Year Update. *J. Manage. Inf. Syst.*, *19*(4), 9–30.

DeLone, W. H., & McLean, E. R. (1992). Information systems success: The quest for the dependent variable. *Information systems research*, *3*(1), 60–95.

Denzin, N. K., & Lincoln, Y. S. (2000). The discipline and practice of qualitative research. *Handbook of qualitative research*, *2*, 1–28.

Denzin, N. K., & Lincoln, Y. S. (2011). *The SAGE handbook of qualitative research*. Sage Publications, Incorporated.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2012). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*. Retrieved from http://www.palgrave-journals.com/ejis/journal/vaop/ncurrent/abs/ejis201223a.html

Donaldson, T., & Preston, L. E. (1995). The Stakeholder Theory of the Corporation: Concepts, Evidence, and Implications. *The Academy of Management Review*, *20*(1), 65–91. doi:10.2307/258887

Donohue, M., & Carblanc, A. (2008). The role of digital identity management in the internet economy: a primer for policymakers. *No. DSTI/ICCP/REG*, *10*.

Dutta, S., & Bilbao-Osorio, B. (2012). The Global Information Technology Report 2012 Living in a Hyperconnected World. 2012: World Economic Forum.

Edward Freeman, R. (2010). Managing for stakeholders: Trade-offs or value creation. *Journal of business ethics*, *96*, 7–9.

Eldon, E. (2009, April 14). Single sign-on service OpenID getting more usage | VentureBeat. Retrieved December 31, 2012, from http://venturebeat.com/2009/04/14/single-sign-on-service-openid-getting-more-usage/

Eom, S. B., & Stapleton, J. (2011). Testing the DeLone-McLean Model of Information System Success in an E-Learning Context. *Student Satisfaction and Learning Outcomes in E-Learning: An Introduction to Empirical Research*, 82.

Esteves, J., & Joseph, R. C. (2008). A comprehensive framework for the assessment of eGovernment projects. *Government Information Quarterly*, *25*(1), 118–132.

Evrensel, A. (2010). Voter Registration in Africa. A Comparative Analysis. Johannesburg: EISA.

Evry, C. (2010). Proof-of-age scheme prepares to expand across Wiltshire. *Wiltshire Times*. Retrieved October 10, 2012, from http://www.wiltshiretimes.co.uk/news/inyourtown/wiltshire/8239556.Proof_of_age_scheme_prepares_to_expand_across_Wiltshire/

Feldman, F. (1970). Leibniz and "Leibniz' Law." *The Philosophical Review*, *79*(4), 510. doi:10.2307/2184291

Fielding, N. G. (1999). The Norm and the Text: Denzin and Lincoln's Handbooks of Qualitative Method. *The British Journal of Sociology*, *50*(3), 525–534. doi:10.2307/592067

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Retrieved from http://trid.trb.org/view.aspx?id=1150648

Flak, L. S., & Rose, J. (2005). Stakeholder governance: Adapting stakeholder theory to e-government. *Communications of the Association for Information Systems*, *16*(1), 31.

Freeman, R. E. (1994). The politics of stakeholder theory: Some future directions. *Business Ethics Quarterly*, 409–421.

Freeman, R. E., Harrison, J. S., & Wicks, A. C. (2007). *Managing for stakeholders: Survival, reputation, and success*. Yale University Press. Retrieved from http://books.google.co.uk/books?hl=en&lr=&id=NJLV1U9gplMC&oi=fnd&pg=PR7&dq=%22Managing+for+stakeholders%22&ots=39BDntgBX3&sig=Wt4YBAsfP5MDf3G8v9DG5QjEUlY

Friedman, A. L., & Miles, S. (2002). Developing stakeholder theory. *Journal of Management Studies*, *39*(1), 1–21.

Friedman, A. L., & Miles, S. (2006). *Stakeholders: theory and practice*. Oxford University Press, USA.

FTC. (2000). A Report to Congress; Fair Information Practices in the Electronic Marketplace.

Gable, G. G., Sedera, D., & Chan, T. (2008). Re-conceptualizing information system success: the IS-impact measurement model. *Journal of the Association for Information Systems*, *9*(7), 377–408.

Gadamer, H. G. (1975). Truth and Method, trans. *W. Glen-Doepel (London: Sheed & Ward)*, 9.

Gambetta, D. (2000). Can we trust trust. *Trust: Making and breaking cooperative relations*, *2000*, 213–237.

Geertz, C. (1973). The Interpretation of Cultures. *New York: HarperCollins Basic Books*, *44*, 70.

GhanaReporters. (2012, December 28). NPP Raises Alarm over 1.3 Million Votes, Takes Massive Evidence to Supreme Court. *Ghana Reporters*. Retrieved December 30, 2012, from http://ghanareporters.com/2012/12/28/npp-raises-alarm-13-million-irregular-votes/

Gibbs, A. (1997). Focus groups. *Social research update*, *19*(8). Retrieved from http://sru.soc.surrey.ac.uk/SRU19.html

Gioia, D. A., & Pitre, E. (1990). Multiparadigm Perspectives on Theory Building. *The Academy of Management Review*, *15*(4), 584–602. doi:10.2307/258683

GNA. (2003, June 11). Electoral Commission To Be Restricted To Conduct Of Elections. *modernghana.com*. Retrieved December 21, 2012, from http://www.modernghana.com/news/35887/1/electoral-commission-to-be-restricted-to-conduct-o.html

Grant, J. A. (2011a). The National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy through Standards. *IEEE Internet Computing*, *15*(6), 80–84. doi:10.1109/MIC.2011.160

Grant, J. A. (2011b). The National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy through Standards. *IEEE Internet Computing*, *15*(6), 80–84. doi:10.1109/MIC.2011.160

Gregory, M. (2012). Philosophy as Prosocial Education. *Handbook of Prosocial Education*, 197.

Grene, M. (1967). Straus's Phenomenological Psychology. *The Review of Metaphysics*, *21*(1), 94–123. doi:10.2307/20124497

Grönlund, \AA, & Horan, T. A. (2004). Introducing e-gov: history, definitions, and issues. *Communications of the Association for Information Systems*, *15*(2004), 713–729.

Gutwirth, S. (2012). European Data Protection: In Good Health? Springer.

Hammer-Lahav, E. (2009, October 16). Beginner's Guide to OAuth – Part I: Overview. *hueniverse*. Retrieved December 31, 2012, from http://hueniverse.com/2007/10/beginners-guide-to-oauth-part-i-overview/

Hardt, D., Bufu, J., & Hoyt, J. (2007). *Openid attribute exchange 1.0-final*. Dec. Retrieved from http://www.immagic.com/eLibrary/TECH/OPENIDUS/O071205E.pdf

Harrison, J. S., Bosse, D. A., & Phillips, R. A. (2009). Managing for stakeholders, stakeholder utility functions, and competitive advantage. *Strategic Management Journal*, *31*(1), 58–74.

Hattori, R. A., & Lapidus, T. (2004). Collaboration, trust and innovative change. *Journal of Change Management*, *4*(2), 97–104.

Heavey, C., & Murphy, E. (2012). A proposed cooperation framework for organisations and their leaders. *Management Decision*, *50*(6), 993–1000. doi:10.1108/00251741211238292

Heidegger, M. (1982). *On the way to language* (Vol. 4023). HarperOne.

Helbig, N., Ramón Gil-García, J., & Ferro, E. (2009). Understanding the complexity of electronic government: Implications from the digital divide literature. *Government Information Quarterly*, *26*(1), 89–97.

Henning, E., Van Rensburg, W., & Smit, B. (2004). *Finding your way in qualitative research*. van Schaik publishers.

IBM. (2010). IBM Research - Zurich | Computer Science | Identity governance. Retrieved October 10, 2012, from http://www.zurich.ibm.com/security/idemix/

Ives, B., & Olson, M. H. (1984). User involvement and MIS success: a review of research. *Management science*, *30*(5), 586–603.

Ives, Blake, & Olson, M. H. (1984). User Involvement and Mis Success: A Review of Research. *Management Science (pre-1986)*, *30*(5), 586.

Jain, A., & Aggarwal, S. (2012). MULTIMODAL BIOMETRIC SYSTEM: A SURVEY. *reason*, *1*(1), 58–63.

Jain, A. K., Bolle, R., & Pankanti, S. (1999). *Biometrics: personal identification in networked society*. kluwer academic publishers. Retrieved from http://books.google.co.uk/books?hl=en&lr=&id=XPC9ucFbddsC&oi=fnd&pg=PR7&dq=Biometrics:+Personal+Identification&ots=zHdkgLb6ZY&sig=x11Y7XkbIhZ7k5yARFK1jqnXugw

Jain, A. K., Flynn, P., & Ross, A. A. (2010). *Handbook of biometrics*. Springer Publishing Company, Incorporated. Retrieved from http://dl.acm.org/citation.cfm?id=1952072

Jamieson, L., & Williams, L. M. (2003). Focus group methodology: explanatory notes for the novice nurse researcher. *Contemporary nurse*, *14*(3), 271–280.

Jiang, J. J., Klein, G., & Discenza, R. (2002). Perception differences of software success: provider and user views of system metrics. *Journal of Systems and Software*, *63*(1), 17–27. doi:10.1016/S0164-1212(01)00135-2

Johnson-George, C., & Swap, W. C. (1982). Measurement of specific interpersonal trust: Construction and validation of a scale to assess trust in a specific other. *Journal of Personality and Social Psychology; Journal of Personality and Social Psychology*, *43*(6), 1306.

Jones, T. M., & Wicks, A. C. (1999). Convergent stakeholder theory. *Academy of management review*, 206–221.

Jøsang, A., & Pope, S. (2005). User centric identity management. In *AusCERT Asia Pacific Information Technology Security Conference* (p. 77). Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.60.1563&rep=rep1&type=pdf

Kaplan, B., & Duchon, D. (1988). Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study. *MIS Quarterly*, *12*(4), 571–586. doi:10.2307/249133

Kitzinger, J. (1995a). Introducing focus groups in qualitative research. *British Medical Journal*, *311*(7000), 299–302.

Kitzinger, J. (1995b). Qualitative research: introducing focus groups. *Bmj*, *311*(7000), 299–302.

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Q.*, *23*(1), 67–93. doi:10.2307/249410

Kramer, R. M. (1999). Trust and distrust in organizations: Emerging perspectives, enduring questions. *Annual review of psychology*, *50*(1), 569–598.

Krueger, R. A., & Casey, M. A. (2009). *Focus groups: A practical guide for applied research*. Pine Forge Press.

Kuhn, T. S. (1996). *The structure of scientific revolutions* (Vol. 2). University of Chicago press.

Laplume, A. O., Sonpar, K., & Litz, R. A. (2008). Stakeholder theory: Reviewing a theory that moves us. *Journal of Management*, *34*(6), 1152–1189.

Laplume, A., Sonpar, K., & Litz, R. (2008). Stakeholder theory: a longitudinal review of a theory that moves us. *Journal of Management*, *24*(6), 1152–1189.

Lee, A. S. (1991). Integrating Positivist and Interpretive Approaches to Organizational Research. *Organization Science*, *2*(4), 342–365.

Lee, C. H., & Cranage, D. A. (2011). Personalisation–privacy paradox: The effects of personalisation and privacy assurance on customer responses to travel Web sites. *Tourism Management*, *32*(5), 987–994.

Lewis, J. D., & Weigert, A. (1985). Trust as a social reality. *Social forces*, *63*(4), 967–985.

Lewis, M. W., & Grimes, A. J. (1999). Metatriangulation: Building Theory from Multiple Paradigms. *The Academy of Management Review*, *24*(4), 672–690. doi:10.2307/259348

Li, S. Z., & Jain, A. K. (2011). *Handbook of face recognition*. Springer. Retrieved from http://books.google.co.uk/books?hl=en&lr=&id=KSXwPmoqGWYC&oi=fnd&pg=PR3&dq=biometrics+handbook&ots=lq4drv7F1i&sig=CKoxoK2zNLBcRxb3aoBWH4kR7b4

Lin, W. S., & Wang, C. H. (2012). Antecedences to continued intentions of adopting e-learning system in blended learning instruction: A contingency framework based on models of information system success and task-technology fit. *Computers & Education*, *58*(1), 88–99.

Lincoln, Y. S., Lynham, S. A., & Guba, E. G. (2011). Paradigmatic controversies, contradictions, and emerging confluences, revisited. *The Sage handbook of qualitative research*, 97–128.

Lips, M., & Pang, C. (2011). Identity management in information age government: exploring concepts, definitions, approaches and solutions. Retrieved from http://researcharchive.vuw.ac.nz/bitstream/handle/10063/1577/article.pdf.txt?sequence=4

Lucas Jr, H. C. (1974). Systems Quality, User Reactions, and the Use of Information Systems. Retrieved from http://www.eric.ed.gov/ERICWebPortal/recordDetail?accno=ED089771

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355.

Malig, C. (1996). *The civil registration system in Denmark*. International Institute for Vital Registration and Statistics.

Mangiuc, D. M. (2012). Cloud Identity and Access Management–A Model Proposal. *Journal of Accounting and Management Information Systems*, *11*(3), 484–500.

Mason, R. O. (1986). Four Ethical Issues of the Information Age. *MIS Quarterly*, *10*(1), 5. doi:10.2307/248873

Maxwell, J. A. (2010). Using numbers in qualitative research. *Qualitative Inquiry*, *16*(6), 475–482.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of management review*, 709–734.

Mayer, Roger C., Davis, J. H., & Schoorman, F. D. (1995a). An Integrative Model of Organizational Trust. *The Academy of Management Review*, *20*(3), 709. doi:10.2307/258792

Mayer, Roger C., Davis, J. H., & Schoorman, F. D. (1995b). An Integrative Model of Organizational Trust. *The Academy of Management Review*, *20*(3), 709. doi:10.2307/258792

McDermott, R. (2012, February 1). Biometric voter verification in Ghana — ACE Electoral Knowledge Network. Retrieved December 30, 2012, from http://aceproject.org/electoral-advice/archive/questions/replies/382803236

McKeen, J. D., & Guimaraes, T. (1997). Successful strategies for user participation in systems development. *Journal of Management Information Systems*, 133–150.

Meredith, J. (1993). Theory Building through Conceptual Methods. *International Journal of Operations & Production Management*, *13*(5), 3–11. doi:10.1108/01443579310028120

Microsoft. (2011, February). Microsoft and U-Prove| End to End Trust | Microsoft Trustworthy Computing. *MICROSOFT U-PROVE CTP RELEASE 2*. Retrieved October 14, 2012, from http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/uprove.aspx

Microsoft. (2013). Windows Live ID; Simplify your sign in. Retrieved January 10, 2013, from https://accountservices.passport.net/ppnetworkhome.srf?lc=2057&mkt=EN-GB$%20id=$i1071$%20target=$_top$$%3Cimg%20src=

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science*, *11*(1), 35–57.

Milne, G. R., & Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy & Marketing*, 206–215.

Modell, S. (2010). Bridging the paradigm divide in management accounting research: The role of mixed methods approaches. *Management Accounting Research*, *21*(2), 124–129. doi:10.1016/j.mar.2010.02.005

Morgan, D. L. (1997). *The focus group guidebook*. Sage Publications, Incorporated.

Morris, M. G., & Dillon, A. (1997). How User Perceptions Influence Software Use. *IEEE Softw.*, *14*(4), 58–65. doi:10.1109/52.595956

Mun, H. J., Yun, H., Kim, E. A., Hong, J. Y., & Lee, C. C. (2010). Research on factors influencing intention to use DMB using extended IS success model. *Information Technology and Management*, *11*(3), 143–155.

Murray, S. A., Kendall, M., Carduff, E., Worth, A., Harris, F. M., Lloyd, A., … Sheikh, A. (2009). Use of serial qualitative interviews to understand patients' evolving experiences and needs. *BMJ*, *339*. Retrieved from http://www.bmj.com/content/339/bmj.b3702?ijkey=e2fb99491f6a48ef6815262c0c36f48d74b8bd72&keytype2=tf_ipsecsha&linkType=FULL&journalCode=bmj&resid=339/sep28_1/b3702

Myers, M. D. (1997). Qualitative Research in Information Systems. *MIS Quarterly*, *21*(2), 241–242. doi:10.2307/249422

NHIS. (2010). SUMMARY STATISTICS AS OF JUNE 2010. Retrieved January 30, 2013, from http://www.nhis.gov.gh/?CategoryID=309

NIA. (2007). Frequently asked questions (FAQs). Retrieved June 30, 2010, from http://www.niaghana. gov.gh

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126.

O'Brien, J., & Marakas, G. (2010). *Management Information Systems*. McGraw-Hill Companies,Incorporated.

OASIS. (2012). OASIS Security Services (SAML) TC | OASIS. Retrieved January 10, 2013, from https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

OECD. (1980). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Retrieved from http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

OECD. (2002). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris: Organisation for Economic Co-operation and Development. Retrieved from http://public.eblib.com/EBLPublic/PublicView.do?ptiID=516205

OECD. (2011a). The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines (OECD Digital Economy Papers No. 176). OECD Publishing.

OECD. (2011b). Education attainment. In *OECD Factbook 2011-2012*. OECD Publishing. Retrieved from http://www.oecd-ilibrary.org/economics/oecd-factbook-2011-2012/education-attainment_factbook-2011-85-en

OECD. (2011c). *Digital Identity Management Enabling Innovation and Trust in the Internet Economy*. OECD Publishing. Retrieved from http://www.oecd.org/sti/interneteconomy/49338380.pdf

Orlikowski, W. J., & Iacono, C. S. (2001). Research commentary: Desperately seeking the" it" in it research—a call to theorizing the it artifact. *Information systems research*, *12*(2), 121–134.

Papamichail, K. N., Alves, G., French, S., Yang, J. B., & Snowdon, R. (2007). Facilitation practices in decision workshops. *Journal of the Operational Research Society*, *58*(5), 614–632.

Pariser, E. (2011). The filter bubble: What the Internet is hiding from you. Penguin Press HC.

Pavlou, P. A. (2011a). State of the information privacy literature: where are we now and where should we go? *Mis Quarterly*, *35*(4), 977–988.

Pavlou, P. A. (2011b). State of the information privacy literature: where are we now and where should we go? *Mis Quarterly*, *35*(4), 977–988.

Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research*, *15*(1), 37–59.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *Mis Quarterly*, *31*(1), 105–136.

Pedersen, C. B. (2011). The Danish civil registration system. *Scandinavian journal of public health*, *39*(7 suppl), 22–25.

Pedersen, C. B., Gøtzsche, H., Møller, J. Ø., & Mortensen, P. B. (2006). The Danish civil registration system: A cohort of eight million persons. *Dan Med Bull*, *53*(4), 441–449.

Pedersen, P. E. (2003). Modifying adoption research for mobile Internet service adoption: Cross-disciplinary interactions. In *36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the*. doi:10.1109/HICSS.2003.1174217

Petter, S., DeLone, W., & McLean, E. (2008). Measuring information systems success: models, dimensions, measures, and interrelationships. *European Journal of Information Systems*, *17*(3), 236–263.

Petter, S., DeLone, W., & McLean, E. R. (2012). The Past, Present, and Future of "IS Success." *Journal of the Association for Information Systems*, *13*(5), 2.

Phillips, R., Freeman, R. E., & Wicks, A. C. (2003). What stakeholder theory is not. *Business Ethics Quarterly*, 479–502.

Pitt, L. F., Watson, R. T., & Kavan, C. B. (1995). Service Quality: A Measure of Information Systems Effectiveness. *MIS Quarterly*, *19*(2), 173–187. doi:10.2307/249687

Pring, R. (2000). The "false dualism"of educational research. *Journal of Philosophy of Education*, *34*(2), 247–260.

Rahaman, A., & Sasse, M. A. (2010). A framework for the lived experience of identity. *Identity in the Information Society*, *3*(3), 605–638.

Rai, A., Lang, S. S., & Welker, R. B. (2002). Assessing the Validity of IS Success Models: An Empirical Test and Theoretical Analysis. *Information Systems Research*, *13*(1), 50–69. doi:10.1287/isre.13.1.50.96

Ratha, N. K., Chikkerur, S., Connell, J. H., & Bolle, R. M. (2007). Generating cancelable fingerprint templates. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, *29*(4), 561–572.

Reay, T., & Whetten, D. A. (2011). What Constitutes a Theoretical Contribution in Family Business? *Family Business Review*, *24*(2), 105–110. doi:10.1177/0894486511406427

Recordon, D., & Reed, D. (2006). OpenID 2.0: a platform for user-centric identity management. In *Proceedings of the second ACM workshop on Digital identity management* (pp. 11–16). New York, NY, USA: ACM. doi:10.1145/1179529.1179532

Ricoeur, P. (1991). Narrative Identity. *Philosophy Today*, *35*(1), 73.

Robey, D., & Farrow, D. (1982). User involvement in information system development: A conflict model and empirical test. *Management Science*, *28*(1), 73–85.

Rojon, C., & Saunders, M. N. K. (2012). Formulating a convincing rationale for a research study. *Coaching: An International Journal of Theory, Research and Practice*, *5*(1), 55–61. doi:10.1080/17521882.2011.648335

Rosen, B., & Jerdee, T. H. (1977). Influence of subordinate characteristics on trust and use of participative decision strategies in a management simulation. *Journal of Applied Psychology*, *62*(5), 628–631.

Rotenberg, M. (2001). Fair Information Practices and the Architecture of Privacy:(What Larry Doesn't Get). *Stan. Tech. L. Rev.*, *2001*, 1–4.

Ruona, W. E., & Lynham, S. A. (2004). A philosophical framework for thought and practice in human resource development. *Human Resource Development International*, *7*(2), 151–164. doi:10.1080/13678860310001630665

Sabherwal, R., Jeyaraj, A., & Chowa, C. (2006). Information System Success: Individual and Organizational Determinants. *Management Science*, *52*(12), 1849–1864. doi:10.1287/mnsc.1060.0583

Sabouri, A., Krontiris, I., & Rannenberg, K. (2012). Attribute-Based Credentials for Trust (ABC4Trust). *Trust, Privacy and Security in Digital Business*, 218–219.

Sarker, S., & Wells, J. D. (2003). Understanding mobile handheld device use and adoption. *Commun. ACM*, *46*(12), 35–40. doi:10.1145/953460.953484

Schaller, R. R. (1997). Moore's law: past, present and future. *IEEE Spectrum*, *34*(6), 52 –59. doi:10.1109/6.591665

Schaupp, L. C., Fan, W., & Belanger, F. (2006). Determining Success for Different Website Goals. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences, 2006. HICSS '06* (Vol. 6, p. 107b). Presented at the Proceedings of the 39th Annual Hawaii International Conference on System Sciences, 2006. HICSS '06. doi:10.1109/HICSS.2006.122

Schutz, A. (1954). Concept and Theory Formation in the Social Sciences. *The Journal of Philosophy*, *51*(9), 257–273. doi:10.2307/2021812

Schwaig, K. S., Kane, G. C., & Storey, V. C. (2006). Compliance to the fair information practices: How are the Fortune 500 handling online privacy disclosures? *Information & management*, *43*(7), 805–820.

Schwartz, P. M. (2000). Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices. *Wis. L. Rev.*, 743.

Scott, M., Golden, D., & Hughes, M. (2004). Implementation Strategies for eGovernment: A Stakeholder Analysis Approach. Retrieved from http://aisel.aisnet.org/ecis2004/101/

Seddon, P. B. (1997). A respecification and extension of the DeLone and McLean model of IS success. *Information systems research*, *8*(3), 240–253.

Seddon, P. B., Staples, S., Patnayakuni, R., & Bowtell, M. (1999). Dimensions of information systems success. *Communications of the AIS*, *2*(3es).

Seltsikas, P., & O'Keefe, R. M. (2010). Expectations and outcomes in electronic identity management: the role of trust and public value. *European Journal of Information Systems*, *19*(1), 93–103. doi:10.1057/ejis.2009.51

Shannon, C. E., & Weaver, W. (1949). The mathematical theory of information.

Sharkey, U., Scott, M., & Acton, T. (2010). The influence of quality on e-commerce success: an empirical application of the Delone and Mclean IS success model. *International Journal of E-Business Research (IJEBR)*, *6*(1), 68–84.

Sharp, L., McDonald, A., Sim, P., Knamiller, C., Sefton, C., & Wong, S. (2011). Positivism, post-positivism and domestic water demand: interrelating science across the paradigmatic divide. *Transactions of the Institute of British Geographers*, *36*(4), 501–515.

Shibboleth. (2013). Shibboleth - About. Retrieved January 10, 2013, from http://shibboleth.net/about/index.html

Shils, E. A., & Finch, H. A. (1949). Max Weber on the methodology of the social sciences. *Glencoe*, *111*, 73ff.

Sinkko, K., Ammann, M., Hämäläinen, R. P., Mustajoki, J., Sinkko, K., Ammann, M., … Mustajoki, J. (2008). Facilitated Workshop A Participatory Method for Planning of Countermeasures in Case of a Nuclear Accident. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.149.9633

Slone, S. (2004). The Open Group Identity Management Work Area. *Identity Management (March 2004)*.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS quarterly*, *35*(4), 989–1016.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS quarterly*, 167–196.

Smith, J. A. (2004). Reflecting on the development of interpretative phenomenological analysis and its contribution to qualitative research in psychology. *Qualitative Research in Psychology*, *1*(1), 39–54. doi:10.1191/1478088704qp004oa

Solove, D. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477.

Solove, D. (2013). Privacy Self-Management and the Consent Paradox. *Harvard Law Review*, *126*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018

Solove, D. J. (2002). Identity theft, privacy, and the architecture of vulnerability. *Hastings Lj*, *54*, 1227.

Sørebø, Ø., & Fuglseth, A. M. (2012). Information Systems Success and Tourism Employees' Use of a Payment System: The Influence of User Motivation, Management Attitude and Ease of Use. *NOKOBIT*, *2012*. Retrieved from http://tapironline.no/fil/vis/1018

Srivastava, S. C., & Teo, T. S. H. (2009). Citizen trust development for e-government adoption and usage: Insights from young adults in Singapore. *Communications of the Association for Information Systems*, *25*. Retrieved from http://halshs.archives-ouvertes.fr/hal-00465199/

Srivastava, Shirish C., & Teo, T. S. H. (2005). Citizen Trust Development for E-Government Adoption: Case of Singapore. In *PACIS'05* (pp. 59–59).

Tashakkori, A., & Teddlie, C. (2010). *Sage handbook of mixed methods in social & behavioral research*. Sage Publications, Incorporated. Retrieved from http://books.google.co.uk/books?hl=en&lr=&id=v4wJF5hZhKgC&oi=fnd&pg=PT1&dq=tashakkori+and+teddlie+2010&ots=SDqWKrUTiH&sig=Xj6P0iMgACsEun0qB04dU1af25Q

Tashakkori, Abbas, & Teddlie, C. (2010). Putting the Human Back in "'Human Research Methodology'": The Researcher in Mixed Methods Research. *Journal of Mixed Methods Research*, *4*(4), 271–277. doi:10.1177/1558689810382532

Taylor, J. A., & Lips, A. M. B. (2008). The citizen in the information polity: Exposing the limits of the e-government paradigm. *Information Polity*, *13*(3), 139–152.

Teddlie, C., & Tashakkori, A. (2012). Common "Core" Characteristics of Mixed Methods Research A Review of Critical Issues and Call for Greater Convergence. *American Behavioral Scientist*, *56*(6), 774–788. doi:10.1177/0002764211433795

Teo, T. S. H., Srivastava, S. C., & Jiang, L. (2008). Trust and Electronic Government Success: An Empirical Study. *Journal of Management Information Systems*, *25*(3), 99–132. doi:10.2753/MIS0742-1222250303

Thorpe, R., & Holt, R. (2007). *The Sage dictionary of qualitative management research*. Sage Publications Limited.

Tidwell, L. C., & Walther, J. B. (2002). Computer-Mediated Communication Effects on Disclosure, Impressions, and Interpersonal Evaluations: Getting to Know One Another a Bit at a Time. *Human Communication Research*, *28*(3), 317–348. doi:10.1111/j.1468-2958.2002.tb00811.x

TNS Opinion & Social. (2011). Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union. *Report. Brussels: European Commission*.

Tolchinsky, P. D., McCuddy, M. K., Adams, J., Ganster, D. C., Woodman, R. W., & Fromkin, H. L. (1981). Employee perceptions of invasion of privacy: A field simulation experiment. *Journal of Applied Psychology*, *66*(3), 308.

Tona, O., Carlsson, S., & Eom, S. (2012). An Empirical Test of DeLone and McLean's Information System Success Model in a Public Organization. Retrieved from http://aisel.aisnet.org/amcis2012/proceedings/StrategicUseIT/10/

Touch2ID. (2012). touch2id - Unlock the city. Retrieved January 12, 2013, from http://touch2id.co.uk/

Treviño, L. K., & Weaver, G. H. (1999). The Stakeholder Research Tradition: Converging Theorists, + Not Convergent Theory. *Academy of Management Review*, *24*(2), 222–227.

Trubow, G. (1992). Personal privacy and secondary-use dilemma (social aspects of automation). *IEEE Software*, *9*(4), 73 –74. doi:10.1109/52.143112

Turkle, S. (1997). Life on the Screen: Identity in the Age of the Internet. Simon and Schuster.

Turner, R. S. (2009). Neo-Liberal Constitutionalism: Ideology, Government and the Rule of Law. *Journal of Politics and Law*, *1*(2), P47.

UNESCO. (2010). *UIS Statistics in Brief; Regional literacy profile - Sub-Saharan Africa*. UNESCO Institute for Statistics. Retrieved from http://stats.uis.unesco.org/unesco/TableViewer/document.aspx?ReportId=367&IF_Language=eng&BR_Region=40540

UNICEF. (2012). UNICEF - At a glance: Ghana - Statistics. *UNICEF*. Retrieved December 14, 2012, from http://www.unicef.org/infobycountry/ghana_statistics.html

Urbach, N., & Müller, B. (2012). The Updated DeLone and McLean Model of Information Systems Success. *Information Systems Theory*, 1–18.

Van Thuan, D. (2007). Identity Management Demystified. *Telektronikk - Identity Management*, *3*(4), 11–18.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management science*, *46*(2), 186–204.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS quarterly*, 425–478.

Venkatesh, Viswanath, Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, *27*(3), pp. 425–478.

Walsham, G. (1995). The Emergence of Interpretivism in IS Research. *Information Systems Research*, *6*(4), 376–394.

Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems*, *15*(3), 320–330. doi:10.1057/palgrave.ejis.3000589

Wang, X., & Xue, H. (2012). The Personal Information Privacy Protection Strategy in Social Security Information System. *Communications and Information Processing*, 718–724.

Wang, Z., Walther, J. B., & Hancock, J. T. (2009). Social Identification and Interpersonal Communication in Computer-Mediated Communication: What You Do Versus Who You Are in Virtual Groups. *Human Communication Research*, *35*(1), 59–85. doi:10.1111/j.1468-2958.2008.01338.x

Warnke, G. (2011). The Hermeneutic Circle versus Dialogue. *The Review of Metaphysics*, *65*(1), 91–112.

Wayman, J., Jain, A., Maltoni, D., & Maio, D. (2005). An introduction to biometric authentication systems. *Biometric Systems*, 1–20.

Weber, M., Shils, E. A., Finch, H. A., & Antonio, R. J. (2011). *Methodology of Social Sciences: Max Weber*. Transaction Publishers.

Webster, J., & Watson, R. T. (2002). Analyzing The Past to Prepare for the Future: Writing a Literature Review. Retrieved from http://www.misq.org/misq/downloads/issue/id/103/

Weiser, M. (1993). Some computer science issues in ubiquitous computing. *Commun. ACM*, *36*(7), 75–84. doi:10.1145/159544.159617

Westfall, J. (2011). Using windows live services. *Windows Phone 7 Made Simple*, 245–260.

Westin, A. F. (1967). *Privacy and freedom*. London [etc.]: The Bodley Head.

Whetten, D. A. (1989). What Constitutes a Theoretical Contribution? *The Academy of Management Review*, *14*(4), 490–495. doi:10.2307/258554

Whitley, E. (2013). On technology neutral policies for e–identity: A critical reflection based on UK identity policy. *Journal of International Commercial Law and Technology*, *8*(2), 134 – 147.

Whitley, E. A. (2009). Informational privacy, consent and the "control" of personal data. *Information Security Technical Report*, *14*(3), 154–159. doi:10.1016/j.istr.2009.10.001

Whitley, E. A., & Hosein, G. (2010). Global Identity Policies and Technology: Do we Understand the Question? *Global Policy*, *1*(2), 209–215. doi:10.1111/j.1758-5899.2010.00028.x

Whitley, E., & Kanellopoulou, N. (2010a). Privacy and Informed Consent in Online Interactions: Evidence from Expert Focus Groups. *ICIS 2010 Proceedings*. Retrieved from http://aisel.aisnet.org/icis2010_submissions/126

Wilton, R. (2008a). Identity and privacy in the digital age. *Int. J. of Intellectual Property Management*, *2*(4), 411–428.

World Economic Forum. (2012a). *Rethinking Personal Data: Strengthening Trust* (No. 300512). Geneva: World Economic Forum. Retrieved from http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf

World Economic Forum. (2012b, October). Unlocking the Economic Value of Personal Data; Balancing Growth and Protection. World Economic Forum. Retrieved from http://www3.weforum.org/docs/WEF_IT_UnlockingValueData_BalancingGrowthProtection_SessionSummary.pdf

Yin, R. K. (2008a). *Case Study Research: Design and Methods*. SAGE Publications.

Yin, R. K. (2011a). *Qualitative research from start to finish*. New York: Guilford Press.

Zallone, R. (2010). The Privacy Paradox or How I Learned to Have Rights that Never Quite Seem to Work. In *AAAI Spring Symposium Series*. Retrieved from http://www.aaai.org/ocs/index.php/SSS/SSS10/paper/viewFile/1116/1516

Part II – List of Selected Papers

Table of Contents

Paper 1

Identification Systems Adoption in Africa; The Case of Ghana.

Joseph, Adjei & Peter, Tobbin

Center for Communication, Media and Information Technologies [CMI]
Aalborg University, Copenhagen,
Lautrupvang 15, 2750, Denmark
Ballerup, Copenhagen

adjei@cmi.aau.dk, tobbin@cmi.aau.dk

Abstract

Several variations of Identity Management Systems are being implemented as an attempt to, curtail incidences of crime and abuse of privacy, and to give citizens easy and seamless access to services. Despite the numerous perceived benefits, a number of challenges hinder successful implementations and adoption in Africa. Using concepts of technology adoption and fit-viability theory, this paper examines the critical factors affecting Identity Management Systems adoption. A framework for IdMS implementation and successful adoption is developed based on the underpinning theories and validated with findings from a survey conducted in Ghana. The proposed conceptual framework would allow organizations and policy makers to determine the critical factors to be considered in future implementation of an identity management system.

1 Introduction

Identity management projects have lately become a major issue capturing media attention and driving how governments interact with citizens, business operations and processes. The arguments by governments for Identity Management systems (IdMS) implementations have generally been to ensure high levels of security, efficiency, cost-effective provision of services, promotion of commercial activity, and ensuring the rights of citizens to informational self determination (Beynon-Davies, 2007). The development of IdMS that is capable of achieving these goals can be a very complex process and will require the cooperation of a number of stakeholders (Aichhlozer & Strauß, 2009). In their paper on understanding complex innovation, Aichhlozer & Strauß, (2009) argue that critical security and privacy systems architecture can be very challenging. This issue presents dilemma to policy makers leading to

their preoccupation with technological features of the systems at the expense of analyzing the wider societal implications of the systems implementation (Lips et al, 2009), (Aichholzer & Strauß, 2009).

In spite of the numerous literature on IdMS implementation, there is a dearth of literature on factors affecting IdMS implementation and adoption from developing countries' perspective. Using a survey conducted in Ghana, we analyze key factors affecting implementations and from which a conceptual framework is developed for future implementations of National IdMS. The subsequent section discusses technological development in Africa and IdMS initiatives in Ghana. Section three discusses the research methodology and brief description of Technology Acceptance Model (TAM) and Fit Viability Theory as used in this paper. In section four, we propose a framework for implementing IdMS from developing countries' perspective and description of the survey in Ghana ending with a discusion of the survey results. In section five we present our conclusions and recommendations for IdMS implementation and adoption.

2 Technological Development in Africa

Many African countries are technologically lagging behind. This has been attributed to several years of primitive cultural practices, bad governance, chaotic climatic conditions, poverty and illiteracy. Historically, natural disasters, landmark events and tribal body marks have been used as means of identification and reference points. These practices, which in the past served their purposes, have in these last days of rapid technological development proved very slow and unreliable, leading to improper forms of identification and authentication, and incorrect demographic statistics. In Botswana, the findings of (Uzoka & Ndzinge, 2009) indicated that biometrics usage is at its infancy despite the fact that industries may be aware of its ability to strengthen security and productivity. The emergence of mobile phones and the tremendous growth in cellular networks have made instant and reliable communication a reality in Africa. Cell phone subscription in Africa rose from 54 million in 2003 to 350 million in 2008 with a forecast average cell phone penetration of 80% by 2012. In Ghana, 80% has already been achieved (GBN, 2010), (Comninos et al, 2008). This growth is driving a gradual shift in Africa towards implementation of various biometrics based identity management and electronic payment systems. Throughout Africa, governments are moving towards various national identity management programs with the enactment of laws. In Ghana, for instance, these include the payment systems Act (ACT662) and National Identification Act (ACT 707), (NIA, 2010). The technological development has however, not come without challenges since there are several accounts of identity frauds. For instance, in Ghana, policy makers, security agencies and the private sector are bedevilled with a particular type of cybercrime popularly

known in Ghanaian parlance as “sakawa”. 419 cybercrimes have already become an international issue in Nigeria (USDoS, 1997).

2.1 Identity & Identity Management Systems

Identity has several dimensions. Psychological identity is the distinguishing characteristics of an individual, whilst social identity refers to the positive self-concept of individuals such as organizational membership, religious affiliation, gender and age group (Tajfel & Turner, 1985). In information systems, identity consists of traits, attributes, and preferences, by which one may receive personalized services either online, on mobile devices, at work, or in many other places (Liberty, 2004). Identity consists of both physical and digital identity. In (Bhargav-Spantzel, Camenisch, Gross, & Sommer, 2007) digital identity may be any kind of characteristics associated to an individual and may take the form of user logins, identity attributes (eye colour, date of birth, etc.) and identifiers (account number, vehicle license plate).

Identity management can mean different things to different people depending on the context (Van Thuan, Identity Management Demystified, 2007). As such existing literature contains several and sometimes overlapping definitions of identity management (IdM) or Identity and Access Management (IAM). In this study, IdM “consists of processes, policies and technologies to manage the complete lifecycle of user identities across a system and to control user’s access to the system resources. In effect technology-based identity management refers to the administration and design of identity attributes, credentials, and privileges (Cavoukian, 2008). Identity Management systems have been used throughout history to establish the basis for trade and governance using different tokens and technologies, seals, coded messages, signatures, and jewelry, etc. (3G_Americas, 2009). IdMS should therefore be a reliable means of identification and authentication of individuals in order to offer them authorized access to resources. Depending on the situation and the context, an individual may be represented by different partial identities (Clauß & Köhntopp, 2001). IdMS helps in acquiring better knowledge about individuals, which is essential in building a certain level of trust. An effective IdMS ensures real-time identification and authentication to distinguish one person from the other. IdMS also assists in the protection of privacy of parties to transactions.

2.2 Identity Management Initiatives in Ghana

In Ghana, several independent IdM initiatives are under way. The National Health Insurance Scheme has already rolled out a nationwide registration by issuing identity cards to beneficiaries. The National Identification Authority is rolling out a biometric based national identi-

fication system, and the Ministry of Interior has introduced a biometric passport. Births and death, voters register, business registrations, social security, drivers and vehicle licensing are other forms of registrations performed by various government agencies in different formats and databases. The government has recently implemented biometric based passports and Drivers and Vehicle License. Adoption has been successful with the main impediment being delays in the issuance of passports or the driving licenses. To enhance commercial activity and to reduce the unbanked and under-banked population in Ghana, a biometric based payment system (e-zwich card) was also implemented by Bank of Ghana (BOG) (Frempong, 2010) whilst the National Identification Authority is in the process of rolling out national identity cards. All commercial banks were directed to reconfigure their existing POS terminals and ATMs to make them e-zwich compatible (Hesse, 2009). These two projects have however failed to live up to expectation and even though the goals seemed laudable from a government point of view (France & Selormey, 2009). According to France & Selormey, (2009) GhIPSS opted for biometric technology because of its superior security in terms of user authentication and its ability to combat card cloning.

3 Methodology

This is a country study research on identification systems from developing countries' perspective. The key question addressed in this paper is, "What factors influence adoption of Identity Management Systems in Developing Countries?". Empirical data were gathered by consulting related studies on Privacy and Identity Management systems adoption and implementation, stakeholder interviews and self-administered questionnaires. Based on the literature review, it became apparent that Davies, (1989) Technology Acceptance Model (TAM), and Fit-viability theory (Tjan, 2001) & (Liang et al, 2007) were relevant to the study since they offered better constructs for this study. Opinions of typical Ghanaian adults were used as the unit of analysis. The questionnaire was designed based on the results of the initial interviews. A multiple-item approach was adopted where each item was measured on a five-point Likert scale, with answers ranging from ''strongly disagree" to ''strongly agree". The result of the analysis forms the basis for the development of the conceptual framework. The research is significant since it addresses identity management issues within the context of developing countries, scarcely represented in the IdM literature.

The items in the questionnaire were developed by adapting existing measures validated by other researchers in IdMS, or by converting the definitions of the construct into a questionnaire format. The questionnaire consisted of five main sections. The questions in section 1 were aimed at gathering demographic information such as gender, age group, occupation, educational background and level of income. Section 2 focused on citizens' perceptions and

understanding of issues like privacy, security and controls in identification systems. Section 3 dealt with perceived usefulness and perceived ease of use. Sections 4 and 5 then focused on economic feasibility and transaction cost. In total, there were 43 questions.

3.1 Technology Acceptance Model (TAM)

Factors affecting technology adoption and diffusion of innovation have been extensively studied with several theories and frameworks haven emanated from it within Information Systems literature. Notable among them are innovation diffusion theory (Rogers, Diffusion of Innovations, 1983), technology acceptance model (TAM) (Davis, 1989) and the unified theory of acceptance and use of technology (UTAUT) (Venkatesh & Davis, 2000). In Davies (1989) TAM for instance, what causes people to accept or reject information technology has been mainly attributed to its perceived usefulness and perceived ease of use. External pressure to adopt has also been identified as another factor affecting technology adoption (Dass & Pal, 2009). Additional factors include complexities, compatibility, relative advantage and all of these theories are aimed at deepening understanding of the factors affecting technology adoption. In Davies, (1989), perceived usefulness describes the degree to which a person believes that an innovation will boost their performance. Perceived ease of use on the other hand describes the degree to which a person believes that adopting an innovation will be free of effort. Where a system is high in perceived usefulness but it requires a great effort from a user, it is beleived that its benefits will be eroded by the efforts required and thereby dissuading users from using it. In effect users are more likely to adopt systems which are easier to use and offer some benefits. These studies have however mainly focused on developed countries. Other factors like free riding, connectivity, and illiteracy that are peculiar to developing countries will also be covered in this study.

3.2 Fit – Viability Model

Liang et al (2007) adapted Tjan's (2001) two dimensional fit-viability model for measuring the extent to which a new technology will fit into the core competence, structure, value and culture of organization and how viable it could be. In their model, Liang et al (2007), defined technology viability as the measure of the extent to which the organizational environment is ready for the application, as well as its economic feasibility, technical infrastructure, and social readiness of the organization. Fit measures the extent to which the technology is capable of meeting the requirement of task. They came with the conclusion that organizations must only pursue applications with good fit and strong organizational viability. Economic feasibility is a key indicator used to measure an organization's readiness to implement technology. The two main criteria for measuring economic feasibility are; cost benefit analysis (e.g. net present value) and transaction cost analysis, where reducing cost can increase customer's

willingness to use a technology (Spraakman, 1997). A high-transaction frequency on the other hand reduces transaction costs and the usage of the application. In effect transaction cost is higher where there is lack of usefulness and ease of use.

4 IdMS Conceptual Framework

TAM has proven to be a very useful tool for understanding and predicting user behaviour in information system implementation since it seeks to place administration and control of information directly into the hands of users. (Aichholzer & Strauß, 2009). The following constructs are therefore adapted from TAM:

Perceived Usefulness: is the degree to which a person thinks that using a particular system will enhance his or her performance. In the case IdMS the focus must br on how users believe identification systems can enhance their day-to-day transactions and interactions. The more of such beliefs, the greater the confidence of users in the system. In effect high perceived usefulness will lead to high intention to accept identification systems.

Perceived Ease of Use: It is the degree to which a person believes that using a particular system will be free of effort (Davis, 1989). In IdM implementations, this consists of the enrolment process, ability to gain access to different services, easy access to support services, etc. In effect high perceived ease of use will encourage users to accept IdMS. Factors such as network anonymization tools, minimum disclosure of personal information, or password managers that securely keep track of different credentials will lead to a high perceived ease of use. (Cavoukian, 2008)

External pressure (Dass & Pal, 2009). Where there is a certain level of force or users require the system to transact business activities, adoption of the system is high. For instance passports are mandatory for international travels and for that matter citizens will be under pressure to adopt a biometric passport.

Privacy*:* Privacy is the right of individuals to decide what information about himself should be communicated to others and under what circumstances (Westin, 1970). It is about people's right to choose how they want to live their life, and what things they want to keep private (De Hert, 2008). In effect privacy refers to the claim or right of individuals to exercise a measure of control over the collection, use and disclosure of their personal information. (Cavoukian, 2008). Users are more inclined to adopt identity management systems which offer a high level of privacy assurance.

Trust: Trust is the state of readiness for unguarded interaction with someone or something. (Tway, 1993). Trust can be influenced by perceptions of intentions and past experiences. In

Ghana for instance many business people perceive that national identifications systems can be used for tax purposes or political witch hunting and will therefore find various means to avoid it. Negative perception on trust can have a direct effect on attitudes towards the system. Therfore high reliability and privacy protection policies will lead to high level of trust.

Fit-Viability: (Tjan, 2001) technology fit issues are qualitative factors that determine to what extent an investment fits with the organization's processes, capabilities and culture. Fit issues are therefore 'internal' factors. In developing countries, such internal factors are literacy rate, the level of political tolerance, infrastructure, cultural norms etc. Viability issues deal with expected return the system is able to generate, such as the value-added potential of the system.

Transaction Cost: Many people are reluctant to pay for government services even if it directly affects their livelihood. Therefore any system requiring high transaction cost is bound to fail in developing countries unless there are no alternatives.

4.1 IdM Adoption Survey in Ghana

In an attempt to determine factors affecting IdMS adoption we conducted a survey using stakeholder interviews and questionnaires. The objective of the interviews was to acquire better understanding of the issues involved in National IdMS implementation, which will influence the design of the questionnaire. The interview focused on key stakeholders in the ongoing National Identification project and the government electronic payment systems (E-Zwich Project). We also interviewed key officials of major commercial banks and trading merchants and two groups of citizens; those who have acquired the E-Zwich cards and those who have not. An interview guide was designed to ensure consistency and to ensure that researchers focus on the IdMS related issues.

In the case of the questionnaire, a group of executive masters in administration (EMBA) participants of Ghana Institute of Management and Public Administration (GIMPA) were selected. This group was selected because they represent a typical group of opinion leaders whose views on national IdMS was the unit of analysis. Additionally I found it to be very cost effective due to budgetary constraints and offered me the opportunity to explain the rationale behind the various questions. 250 questionnaires were administered and 230 responses were received and analysed. The following key constructs stated in 4 above were used to develop the questionnaire.

4.2 Results and Discussion

Based on employment positions, 95% of the candidates occupy managerial positions. Even though National Identity (NID) Cards system encounter a lot of opposition in western coun-

tries, particularly the US and the United Kingdom, 90% of respondents believed that NID cards must be compulsory for all Ghanaians and that the cards can be forged. Another interesting finding was that 80% of respondents prefer that cards be issued to citizens free of charge as a means of universal coverage and forgery prevention. Another interesting finding from the survey was that the respondents were unanimous in their responses to questions on governance, policy and monitoring. For instance, they all believed that their interest would be considered in deciding how identity data is used which is consistent with Davis (1989) suggestion that the design characteristics of a system exert immediate effects on perceived usefulness as well as indirect effects via perceived ease of use.

Even though security is a major concern in the West, in this survey respondents rather believed that the system will be secure and for that matter their personal data will not be affected even though they believed there are some risks involved due to lack of competent personnel to manage the databases. Concerning complexity in the use of the cards, majority of the respondents did not think it would be very difficult to use. A further probe however indicated that this belief stems from the fact that respondents have all used ATM cards and thought the NID cards even in its advanced form may not be anything different. They also believed that the introduction of the identity cards will not have any negative impact on users' personal information and that they were prepared to trade off some privacy for convenience, security and faster access to public service. Strangely, all the respondents were willing to allow identification authorities to share their personal data with other government agencies and private businesses. The analysis showed that among those who did not want identifications systems to reveal their identity 90% were business owners. Where IdMS are required for key business activity to take place, adoption is usually high (e.g. passport and health insurance card).

5 Conclusion and Recommendation

This paper has identified factors influencing the adoption of IdMS and its implementation from developing countries' perspective. It has shown that security issues, privacy and anonymity, which are very critical to developed countries, are not the major concerns of those in developing countries. Rather, costs of equipment, tax implications and political issues were the key factors. On the other hand perception of political and taxation motives were seen as key factors that can inhibit the sustainability of the system. This implies that to achieve high levels of IdMS adoption, policy makers must go beyond perceived usefulness and ease of use. Citizens must have confidence in the system without any hidden motives. Again IdMS implementations can be successful in Africa if they are associated with mandatory systems like passports and driving licences. Therefore, policy makers and businesses must be careful in dealing with the inhibiting factors, if future IdMS implementations are to be successful.

Acknowledgements

We would like to thank Professor Henning Olesen, CMI, Aalborg University for his helpful comments during the development of the paper.

References

3G_Americas. (2009). Identity Management; overview of standards & technologies for mobile and fixed internet. 3G America whitepaper.

Aichhlozer, G., & Strauß, S. (2009). Understanding a Complex Inovation process: Identity Management in Austrian E-Government. The Proceedings of the 10th International Digital Government Research Conference.

Aichholzer, G., & Strauß, S. (2009). The Citizens Role in National Electronic identity Management: A Case-study of Austria. Second international Conference on Advances in Human-Oriented and Personalized Mechanisms, Technologies, and Services. Porto, Portugal.

Beynon-Davies, P. (2007). Personal identity management and electronic government; the case of the national identity card in the UK. Journal of Enterprise Information Management , Vol. 20 (No.3), 244-9.

Bhargav-Spantzel, A., Camenisch, J., Gross, T., & Sommer, D. (2007). User centricity: a taxonomy and open issues. 15.

Cavoukian, A. (2008). The case for privacy-embedded laws of identity in the digital age. Technical report.

Clauß, S., & Köhntopp, M. (2001). Identity Management and its support of multilateral security. Computer and Networks , 37, 205-219.

Comninos, A., Esselaar, S., Ndiwalana, A., & Stork, C. (2008). Towards Evidence-based ICT Policy and Regulation M-banking the Unbanked;. Policy Paper 4, IDRC.

Dass, S., & Pal, S. (2009). Feasibility and Sustainability Model for Identity Management. India: IIMA Research and Publications.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly , 13 (3), 319-340.

De Hert, P. (2008). Identity management of e-ID, privacy and security in Europe: A human rights view. Information Security Technical Report (13), 71 – 75.

FIDIS. (2007). Future of Identity in the Information Society: A Survey on Citizens' trust in ID systems and authorities.

France, F., & Selormey, D. (July/August 2009). Biometrics improving financial accessibility. Biometric Technology Today , S. 10-11.

Frempong, B. (Wed, 28th . April 2010). E-zwich is the dominant money transfer system in Ghana . Von Citifmonline.com: http://www.citifmonline.com/site/business/news/view/5232/3 abgerufen

GBN. (2010). Ghana's mobile penetration expected to hit 100% in 2013. Von http://www.ghanabusinessnews.com/2010/06/08. abgerufen

Hardin, G., & Baden, J. (1977). Managing the Commons. San Francisco: Freeman.

Hesse, D. A. (2009). The e-zwich electronic clearing and payment system. Financial and corporate Ghana 2009 Edition , S. 383.

Liang, T., Huang, C., Yeh, Y., & Lin, B. (2007). Adoption of mobile technology in business: a fit-viability model. Industrial management & data systems , 107 (8), 154-169.

Liberty. (2004). Whitepaper: Benefits of Federated Identity to Government. Liberty Alliance Project.

Lips, A. M., Taylor, J. A., & Organ, J. (2009). Managing Citizen Identity Information in EGovernment Service Relationships in the UK. Public Management Review, , 11 (6), 833 - 856.

NIA. (2010). National Identification Authority. Editorial; NIA News , 1.

Rogers, E. (1983). Diffusion of Innovations (third ed Ausg.). New York: The Free Press.

Spraakman, G. (1997). Transaction cost economics: a theory for internal audit? Managerial Auditing Journal , 12 (7), 323–330.

Tajfel, H., & Turner, J. C. (1985). The social identity theory of intergroup behavior. In S. W. Austin, Psychology of intergroup relations (Bd. 2nd, S. pp. 7-24). Chicago: Nelson-Hall.

Tjan, A. (2001). Finally, a way to put your internet portfolio in order. Harvard Business Review , Vol. 79 (No. 2), pp. 76-85.

Tway, D. C. (1993). A Construct of Trust, Dissertation.

USDoS. (1997). Nigerian Advance Fee Fraud. United States Department of State Bureau of International Narcotics and Law Enforcement Affairs.

Uzoka, F.-M. E., & Ndzinge, T. (2009). Empirical analysis of biometric technology adoption and acceptance in Botswana. The Journal of Systems and Software , 82, 1550–1564.

Van Thuan, D. (2007). Identity Management Demystified,,. 3 (4).

Venkatesh, V., & Davis, F. (2000). A theoretical extension of the technology acceptance model: four longitudinal field studies. 46 (2), pp. 186–204.

Westin, A. (1970). Privacy and Freedom. New York: Atheneum.

Paper 2

Analysis of Privacy-Enhancing Identity Management Systems

Joseph K. Adjei and Henning Olesen

Center for Communication, Media and Information Technologies (CMI)
Aalborg University Copenhagen
Lautrupvang 1A, 2750 Ballerup, Denmark
E-mails: {adjei, olesen}@cmi.aau.dk

Abstract— Privacy has become a major issue for policy makers. This has been impelled by the rapid development of technologies that facilitate collection, distribution, storage, and manipulation of personal information. Business organizations are finding new ways of leveraging the value derived from consumer information. On the other hand, consumers have expressed concerns that their rights and ability to control their personal information are violated. Paradoxically, it appears that users provide personal data freely and willingly, as it has been observed on Facebook and other social networks. This study is an attempt to understand the relationship between individuals' intentions to disclose personal information, their actual personal information disclosure behaviours, and how these can be leveraged to develop privacy-enhancing identity management systems (IDMS) that users can trust. Legal, regulatory and technological aspects of privacy and technology adoption are also discussed.

Keywords—Privacy, Trust, Identity, Identity Management

INTRODUCTION

Incidences of cyber fraud and abuse of privacy on the Internet can have serious consequences for electronic business and the users' trust in performing online transactions. When security is breached, it also endangers user privacy and trust in institutions. Such security breaches have contributed to a growing desire for efficient and cost-effective measures in the design and administration of IDentity Management Systems (IDMS).

Several governmental and business initiatives seek to place the administration and control of identity information directly in the hands of individuals. These initiatives are aimed at curtailing security breaches and abuses of privacy in order to boost user confidence in online trans-

actions and interactions. They require that individuals be given the right to exercise control over the collection, use, and disclosure of their personal information – their digital personae. Previous researches have proposed Fair Information Practice (FIP) principles, Privacy by Design (PbD) and The Seven Laws of Identity (Cameron, The Laws Of Identity, 2005), [2], and [3]. These proposed frameworks and best practices seek to balance an individual's right to privacy with the organization's legitimate need to collect, use, and disclose personal information. Such attempts to give users the latitude to their digital identities are generally referred to as user-centric.

Unfortunately, researchers and developers of user-centric IDMS have mainly focused on making existing IDMS architectures interoperable, while privacy should actually be at the core of the IDMS design. Again, there is the perception that even though individuals advocate for their privacy, they have little or no reservations in releasing their personal information in social networks (e.g. Facebook).

This so-called “privacy paradox” is what motivates our study. Furthermore, many of the current initiatives are focused on online solutions and services in the digital world, but identity management also needs to take into account differences between users’ behaviour in the physical and the digital world. The objective of this work is therefore to understand the major issues involved in the design of privacy-enhancing IDMS and contribute to improved framework and design principles for these.

The paper analyses existing international privacy regulations and the proposed standards and best practices in view of Technology Acceptance Model (TAM) [4]. The remaining part is divided into five sections. Section II contains definitions and concepts and gives a review of research on identity management, privacy and trust. In Section III, some of the major frameworks, initiatives and best practices are presented and compared. Section IV deals with privacy enhancing technologies for authentication and authorization, in particular U-Prove and OAuth. In Section V we present an updated framework and discuss the requirements and guidelines for realizing privacy-enhancing identity management, and finally, Section VI summarizes our findings and conclusions and give some recommendations for future studies.

IDENTITY MANAGEMENT, PRIVACY AND TRUST

The objective of this work is to understand the major issues involved in the design of privacy-enhancing IDMS. This is based on the premise that designing privacy enhancing technology is not just a technological problem but theoretical, social and regulatory dimension must also

be addressed. The research problem then is "What factors must be considered in designing privacy-enhancing IDMS that address both online and offline identity management issues?". To address the research question we analysed the major privacy and data protection regulations, research initiatives, privacy-enhancing technologies in the light of technology acceptance model.

Identity and Identity Management

Identity in information systems consists of traits, attributes, and preferences, based on which an individual may receive personalized services. These services could be online, on mobile devices, or face-to-face (Liberty, 2004). In essence, identity has both physical and digital dimensions. Digital (or electronic) identity is therefore an electronic representation of a real-world entity or an online equivalent of an individual (Roussos, Peterson, & Patel, 2003). Traditionally, IDMS are ran by organizations that control all mechanisms for authentication (establishing confidence in an identity claim's truth) and authorization (deciding what an individual should be allowed to do), as well as any behind-the-scenes profiling or scoring of individuals [5].

In this study, we adopt the Van Thuan (2007) definition of IDMS as "consisting of processes, policies and technologies used to manage the complete lifecycle of user identities across a system and to control the user access to the system resources by associating their rights and restrictions".

To ensure protection of privacy, security and provision of trusted services, different variations of IDMS were used throughout history to establish the basis for trade and governance by means of tokens and technologies, seals, coded messages, signatures, jewellery, etc. (3G_Americas, 2009). There has been a tremendous growth in online government services, business transactions and social interactions via single sign-on (SSO) (Aichholzer & Strauß, 2009). Such activities require efficient and effective user identification and authentication, making IDMS very challenging. Clarke (1994) posits that identification is *"the association of data with a particular human being"*. Authentication is a process that results in a person being accepted as authorized to engage in or perform some activity (Whitley, 2009). Lips (2008) suggested a shift in focus towards analyses of the wider societal implications of IDMS implementation and related social design issues.

Concepts of Privacy

Privacy refers to the claim or right of individuals to exercise a measure of control over the collection, use and disclosure of their personal information. Westin (2003) described privacy concern as customers' apprehension over the acquisition and use of their personal data.

Until recently, personal identity and privacy were something of which each human being could exercise a reasonable degree of control [6]. With the advent of the Internet and high-speed communication technologies, it has become an illusion for users to assume physical control over the collection and use of their personal information since data can be mishandled. For example in many instances, users have little or no involvement the dissemination of their personal information. In essence, mishandled personal information puts individuals' privacy interests at risk.

It is for this reason that governments must protect their citizens. Interestingly, many of the present privacy legislations in Europe were drafted on the basis of the Strasburg Convention of 1981 [6]. Therefore, legislation does not adequately assist in resolving contemporary privacy intrusion cases.

Furthermore, what constitutes personal information has comparatively widened due to increased usage of digital media for business and social interactions, e.g. user names, passwords, etc. Moreover, the concept of privacy has both collective and individual dimensions [7]. Hence, privacy cannot be conceptualised as autonomy from collective norms. This is what informs the debate on whether privacy protection is best approached on the basis that it is a private good or a common good [8]. The rights and obligations of individuals in many countries have therefore been weighed against the collective security and public safety goals – particularly in the USA and UK [8].

Concepts of Trust

Privacy concern has far-reaching effects on individuals' attitudes towards IDMS. Where there is the concern of vulnerability, people become apprehensive towards the systems. According to the Oxford Dictionary, trust is the belief that somebody or something is good, sincere, honest, etc., with no intention to harm or trick. There are different research positions on what constitutes trust and on the outcomes of trust [9]. In the literature, trust has been defined as the confidence in an exchange partner's reliability and integrity [10]. This confidence provides the basis for customers to believe in the reliability and integrity of organizations. It is one of the building blocks for information sharing. Milne & Boza (1999) and Norberg et al.

(2007) examined how privacy concerns are related to trust. They have suggested that increasing trust can mitigate privacy concern.

In Mayer et al. (1995) trust is conceptually distinct from the behaviours that may or may not reflect it. Without a clear distinction between the behaviours the difference between trust and similar constructs is blurred. For instance, Mayer et al. conceptualized trust as *the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other party will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party.*

Effectively, in a trustworthy relationship, individuals are motivated to share personal information freely with no fear of exploitation. Hence, trust can influence both positive and negative behaviour of people. This claim is shared by Jøsang & Fabre in [11]. They observed that the basic ingredients of trust are: 1) dependence on the trusted party, 2) reliability of the trusted party, and 3) risk in case the trusted party does not perform as expected. This implies that trust requirements have direct correlation with risk exposure.

In the study conducted by Mayer et al., three important characteristics of trust were revealed: Ability, benevolence and integrity. Ability also implies competence or perceived expertise. Consistency, fairness and reliability were also used to describe integrity whereas loyalty, openness and availability were used to describe benevolence. These trust characteristics are adopted in this study as the constructs of trust.

The Privacy Paradox

In many privacy scenarios, commercial interests seek to maximize the value of consumer information. For instance, many websites that provide useful information also require users to register in order to access the information. Even though individuals may be willing to part with personal information in order to realize the perceived benefits, many express concern about the violation of their rights and ability to control their personal information.

If we had perfect identity, security would not be an issue, just as systems with perfect anonymity will not present any privacy problem. In spite of the complaints, common use of Facebook, Twitter, etc., indicates that consumers quite often freely release personal data in their interactions and business transactions [12]. This is referred to as “The Privacy Paradox” [12], [6]. Privacy paradox is the relationship between individuals’ intentions to disclose personal information and their actual personal information disclosure behaviours.

An IBM 2008 survey suggests that individuals see a trade-off between the increased value of services and the consequent erosion in their privacy [13]. Consumers are on the one hand seeking for online experience devoid of fraud, cheaper and more conveniently delivered. Yet, there are fears that this could lead to an erosion of users' privacy. In essence, technology has a dual nature: User empowerment and raising security and privacy concerns.

Technology Acceptance Model (TAM)

Factors affecting technology adoption have been extensively studied in the Information Systems literature. Morris & Dillon (1997) posit that user acceptance is "the demonstrable willingness within a user group to employ information technology for the tasks it is designed to support". Notable research on adoption and diffusion of technology includes Innovation Diffusion Theory (Rogers, 1983), TAM (Davis, 1989) and the unified theory of acceptance and use of technology (UTAUT) (Venkatesh & Davis, 2000).

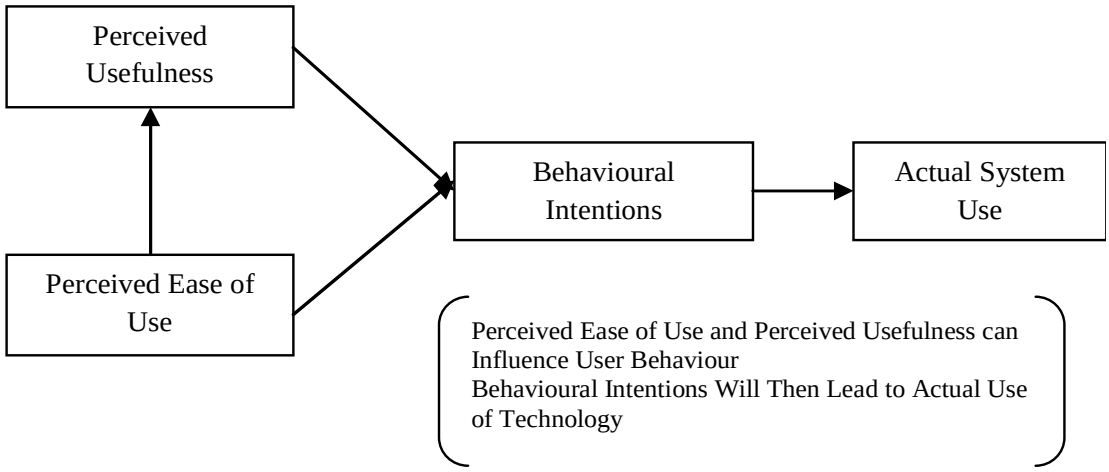


Fig. 1. Main elements of the Technology Acceptance Model *(Adapted from* [4]*)*.

In Davis (1989) perceived usefulness (PU) and perceived ease of use (PEOU) were theorized to be fundamental determinants of behavioural intentions to accept or reject information technology, cf. Fig. 1. Perceived usefulness essentially describes the degree to which a person believes that an innovation will boost their performance (Davis, 1989). Perceived ease of use on the other hand describes the degree to which a person believes that adopting an innovation will be free of effort. In effect, users are more likely to adopt systems, which are easier to use and offer some benefits, since these two factors can affect the behavioural intention to consid-

er using it and actually using the innovation. Behavioural intentions are formed on the basis of an individual's attitude, subjective norms, and perceived control of an outcome [14].

Perceived usefulness, perceived ease of use and behavioural intentions will have already been proven to be a reliable means for determining adoption of technology [4], [15]. This study introduces aspects of trust and privacy in the design of privacy-enhancing IDMS. This is based on the premise that users will feel comfortable with systems that protect their privacy and are more likely to release personal information to only trusted third parties – the essence of user centricity [16].

FRAMEWORKS AND INITIATIVES

Regulatory Framework on Privacy

Motivations for good behaviour can generally be analysed based on the risk of data disclosure and regulatory exposure. Regulation in this regard can be categorized into national and international. The Fair Information Practice principles (FIP) are a set of such principles developed in the 1970s, which has been adopted by many government agencies, public interest groups, and private companies around the world [5]. The Organization for Economic Cooperation and Development (OECD) issued a set of data protection guidelines, which are an adaptation of FIPs. These guidelines focus on privacy as personal data flows between member countries. It addresses the collection and use of personal data, such as names, addresses, government-issued identifiers, etc.

The OECD guidelines are very instructive for design of privacy-enhancing IDMS. The key sections are as follows (OECD):

- *Collection limitation.* Limits to the collection of personal data should exist. Personal data should be collected by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject (the individual).
- *Data quality.* Personal data should be relevant to the purposes for which it is collected and used. It should be accurate, complete, and timely.
- *Purpose Specification Principle.* The purpose for which personal data are collected must be specified no later than at the time of date collection and subsequent use must be limited to the fulfilment of those purposes or such others as are not incompatible with the original purpose and as are specified on each occasion of change of purpose.
- *Use limitation.* Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.
- *Security.* Reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification and disclosure should protect personal data.

- *Openness.* The existence of systems containing personal data should be publicly known, along with a description of the system's main purposes and uses of the personal data in the system.
- *Individual Participation.* An individual should have the right: a) to obtain confirmation from a data controller, or otherwise, any information relating to them within a reasonable time. The cost of obtaining such information must be reasonable and in a form that is readily intelligible to him.
- *Accountability.* The keepers of personal data should be accountable for complying with fair information practices. These principles are the logical starting point for anyone designing an identity management system.

There are also various country- (or region-) specific laws on privacy that seek to protect privacy. In Europe for instance, many of the privacy and data protection laws have been brought together as a harmonized European Union (EU) data protection directive. All EU member states are required to comply. The Directive provides mechanisms to track misuse of personal data and protection against the misapplication of personal data [18]. Unlike the FIPs, breaching legislations and directives can result in prosecution in courts.

The major defects of the regulatory framework are twofold. In the first place, FIPs originated long before the World Wide Web and the digital age [5]. Hence, they are inadequate in dealing with modern privacy since acquisition and use of personal information occurs in microseconds and usually with no direct involvement of parties. Secondly, on the Internet, there are no specific border demarcations, making it difficult to enforce country- or region-specific laws on privacy and data protection. This is because culprits might not be nationals of the countries, where the incidence occurred (e.g. the WikiLeaks cases).

User-Centric Identity Management Systems

The focus on users' quest for power to exercise informational self-determination has resulted in several user-centric and claims-based IDMS initiatives (PrimeLife, 2009), (FIDIS, 2007), (Cameron, 2005). User-centric IDMS is an approach to give users greater control over their personal information. However, the notion of user centricity does not imply a trade-off between security and usability, but rather a focus on user's privacy and trust. For instance, in their Austrian IDMS study, Aichholzer & Strauß (2009) identified equality of access, privacy protection and user convenience as major factors determining users' acceptance of IDMS. Cameron's Seven Laws of Identity have therefore been widely regarded as a guide for providing user-centric IDMS solutions. Generally, the laws of identity prescribe the need for con-

sistent user experiences in online transactions, user understanding, user choices and control, and minimum disclosure of user information to only the intended parties.

Identity providers therefore act as trusted third parties to store user accounts and profile information and authenticate users (OECD, The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers, 2009). Service providers on the other hand accept assertions or claims about users from the identity providers. Since identity providers do not form a federation in a user-centric IDMS model they are seen as operating in the interest of users instead of the service providers (also called "relying parties").

A feature in user-centric IDMS, which makes them more privacy enhancing, is the fact that users have the privilege of choosing what information to disclose when dealing with service providers in particular transactions and still satisfy the need to provide certain information the transaction requires (OECD, The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers, 2009), [20].

Privacy Research Initiatives

To address the inefficiencies of regulations discussed above, a wide range of industry, academic, and governmental organizations in Europe joined forces in a number of research projects, among these "*Privacy and Identity Management for Europe (Prime)*", and "*Privacy and Identity Management in Europe Throughout Life (PrimeLife)*" [21]. These projects have developed working prototypes of privacy-enhancing IDMS, These EU initiatives provide very good frameworks for building privacy-protecting IDMS, although they do not cover US specific regulations.

Kim Cameron, Microsoft Identity Architect, and Ann Cavoukian, Ontario's Information Privacy Commissioner, have done a lot of research on privacy, which is becoming industry standard. In her paper, "7 Laws of Identity: The Case for Privacy-Embedded Laws in the Digital Age," Cavoukian (2008) offered a unique interpretation of Cameron's Laws of Identity. Cavoukian further proposed seven foundational privacy principles, referred to as Privacy by Design (PbD) principles. Her proposal was based on the notion that innovation, creativity and competitiveness must be approached from a design thinking perspective [22]. In a separate study, Peter Schaar posits that "PbD is adjuvant for all kinds of IT systems designated or used for the processing of personal data. It should be a crucial requirement for products and services provided to third parties and individual customers." [3]. Table I provides a summary of the seven laws of identity, the FIPs and Cavaokian's PbD.

TABLE I

MAPPING OF THE LAWS OF IDENTITY, PRIVACY BY DESIGN AND THE FAIR INFORMATION PRACTICES

Seven Laws of Identity	FAIR INFORMATION PRACTICES (FIP)	PRIVACY BY DESIGN
1 – User Control and Consent: Technical identity systems must only reveal information identifying a user with the user's consent	Collection limitation	Privacy as the default setting
2 – Minimal Disclosure for a Constrained Use: The identity metasystem must disclose the least identifying information possible, as this is the most stable, long-term solution.	Data quality	Privacy as the Default Setting
3 – Justifiable Parties: IDMSs must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.	Purpose Specification Use limitation.	Privacy as the default setting
4 – Directed Identity: A universal identity meta system must support both "omnidirec-		End-to-End Security

The seven laws of identity also describe the basis for a "unifying identity metasystem" that can be applied to identity on the Internet. The Identity Metasystem is an interoperable architecture for digital identity, which assumes that users will have several digital identities based on multiple underlying technologies, implementations, and providers (Cameron, The Laws Of Identity, 2005). It ensures that not only are individuals in control of their identity, but also

organizations will be able to continue to use their existing identity infrastructure investments, choose the identity technology that works best for them, and more easily migrate from old technologies to new technologies without sacrificing interoperability with others (Cameron, The Laws Of Identity, 2005).

The major informational privacy [23] emanating from digital identities in the identity meta-system are observability and linkability. Observability is the possibility that others, including communicating parties, service providers, eavesdroppers and third parties will gain information. Linkability on the other hand describes the possibility of linking different data or data sets to an individual for further analysis.

PRIVACY-ENHANCING TECHNOLOGIES

The move to online services offers great promise in terms of both cost reduction and improved user experience. However, the realization of this promise has been severely hampered by the lack of trust on the Internet – specifically, the absence of a practical mechanism for users to obtain and present strong, verified digital identity information online. In some cases, the information simply is not available in a digital form; however, even when it is available, the current set of identity technologies force a trade-off between the level of identity information assurance that can be achieved and the level of privacy given to users. Further, the user‘s experience for providing this information is often inconsistent and difficult, and sometimes redundant.

TABLE II

ANALYSIS OF U-PROVE AND OAUTH IN THE LIGHT OF THE USER-CENTRIC SOLUTIONS

DESCRIPTION	U-PROVE	OAUTH
Purpose of the Application	Designed for Electronic Transactions and Communication	For information sharing on the internet
Coverage		Video, Photos and Contact List
Minimal Disclosure		
Trust	Uses Cryptography	Does not use Cryptography
User Control & Consent	Does not allow profiling	Users can grant 3rd access personal resources without sharing password
Privacy		
Perceived Trust		
Pluralism of Operators and Technologies		OAuth works on Desktop Applications

Digital identity must embrace both being public and being private by providing both anonymity and pseudonymity. It always exists in a context, and we expect the context to have the same degree of separation, which we are used to in the natural world, even though space and time no longer serve as insulation.

In a user-centric IDMS, the issue of distrust between the user and the relying party is addressed, because the identity provider acts as a trusted third-party broker. This occurs because individuals may have several identity providers and for that matter, their information may not be stored in one place. Users will naturally trust brokers they can control whereas relying parties will not trust a broker if the claims asserted are actually self-vouched by the user [16], (OECD, The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers, 2009).

This is what the U-prove and OAuth technologies seek to address by managing claims and attributes so that relying parties are assured that the information is correct before engaging with the user, without necessarily revealing the identity of the user. This approach will still leave the user in control. U-Prove and OAuth enable the use of services with minimum dis-

closure of personal information and fine-grained delegation of authorization between service providers. Some of their features are summarized in the following.

U-Prove

U-Prove is an advanced cryptographic software designed for electronic transactions and communications to overcome a long-standing dilemma between identity assurance and privacy already mentioned (OECD, The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers, 2009), (Microsoft_Connect, Microsoft U-Prove Community Technology Preview R2, 2010). The technology is part of Microsoft's drive to promote an open identity and access model for individuals, businesses and governments, based upon the principles of the identity metasystem (Cameron, The Laws Of Identity, 2005).

The dilemma is addressed by enabling minimal disclosure of identity information in electronic transactions and communications. To ensure minimum disclosure the U-Prove Agent software acts as an intermediary between websites. This allows users to share data in a manner that protect their privacy, since they can now choose to share or otherwise. U-Prove includes a mechanism that separates the retrieval of information from trusted third parties from the release of this information to the destination site. This implies that the organization issuing the information is prevented from tracking where or when information is used. The destination site is similarly prevented from linking users to their activities.

OAuth

Open Authorisation (OAuth) is an open standard for authorization, which gives users the ability to grant third-party access to their resources without sharing their passwords [25]. It also provides a way to grant limited access (in scope, duration, etc.). OAuth allows users to share their private resources (e.g. photos, videos, contact lists, bank accounts) stored on one site with another site without having to hand out their credentials, typically username and password. The concept of OAuth is based on the metaphor of a valet key of car, since it only gives third parties a controlled (limited) access to the car [26], [25]. OAuth mimics the valet key metaphor by providing sites with just enough information to accomplish what the user has requested, but not allowing third-party sites access to any other user information. Precisely, it only allows users to hand out to third parties tokens (instead of credentials) to their data hosted by a given service provider. The tokens could be granting a printing service access to photos without sharing username and password. OAuth 2.0, which is the latest version, focuses

on client developer simplicity (not user simplicity) while providing specific authorization flows for web and desktop applications, mobile phones, and living room devices [25].

Table II presents some of the main features of U-Prove and OAuth and compares them with the privacy design principles discussed above.

IMPROVED FRAMEWORK AND GUIDELINES

The fact that present privacy laws are based on principles drafted many years ago, when the web did not exist, shows that privacy legislation need to make a quantum leap to be in line with the realities of today's real life operating environment. In cyberspace, there are no clear visual cues about the level of privacy available [7]. Existing privacy legislations and regulations do not adequately deal with digital identity issues, because laws are country- or region-specific, and the FIPs are not laws.

Important privacy considerations are in relation with data collection, data usage, storage, data minimization, anonymity, pseudonymity, and the extent to which individuals have control over their personal information. Generally, identity systems that facilitate anonymity and pseudonymity may offer better promise of privacy. In essence, to ensure privacy, risk of vulnerability, the lifespan of identity information, and the costs of processing, storage and deletion are critical.

Linking identities that do not share the same degree of anonymity, or that contain different sets of attributes may allow others to overcome pseudonyms and discover the user's identity. Differences may arise as to which practices of identity and other data collection, use, and retention can be left to market forces and those that should be the subject of government intervention. Controlling linkability involves both maintaining separate contexts so observers cannot accumulate sensitive data and being cautious when identity information is requested to keep track of information disclosure [5].

Since much of the literature on privacy enhancing initiatives aims at introducing technologies with the user in mind it was apparent that the analysis is carried out in the light of Technology Acceptance Model. For instance if privacy must be at the core of the design [22], then obviously the original TAM must be extended to include privacy as a construct. Likewise, to address the dilemma between identity assurance and privacy, trust must also be added as a construct.

We therefore propose to add Perceived Privacy and Perceived Trust as constructs to the original TAM, cf. Fig. 2. As shown in the diagram Perceived Usefulness, Perceived Ease

of Use, Perceived Trust and Perceived Privacy will affect users' behavioural intentions and in the end their decision to conveniently use the IDMS.

IDMS having privacy design flaws can generate adverse consequences for consumers, including the risk of identity theft. On the contrary, IDMS can play a privacy protective role, particularly in the context of social interactions.

TABLE III
FACTORS TO BE CONSIDERED IN THE DESIGN OF PRIVACY-ENHANCING IDMS

Item	MEASUREMENT CRITERIA	Description
Perceived Usefulness	Ease of Use Enhanced Security Identity Fraud prevention Data Quality	Perceived usefulness describes the degree to which a person believes that an innovation will boost their performance
Perceived Ease of Use	User-Centricity Universal Coverage (Online/Offline)	Perceived ease of use describes the degree to which a person believes that adopting an innovation will be free of effort.
Perceived Privacy	Best Practices Regulations, Privacy by design	Application of Laws, Regulations and the laws of identity (see table 2)
Perceived Trust	Ability	The group of skills, competences

On the basis of this extended theoretical framework recommendations for improved design of privacy-enhancing IDMS can be derived. Table III is a summary of the major items, which must be taken into consideration during the design of privacy-enhancing technologies. For

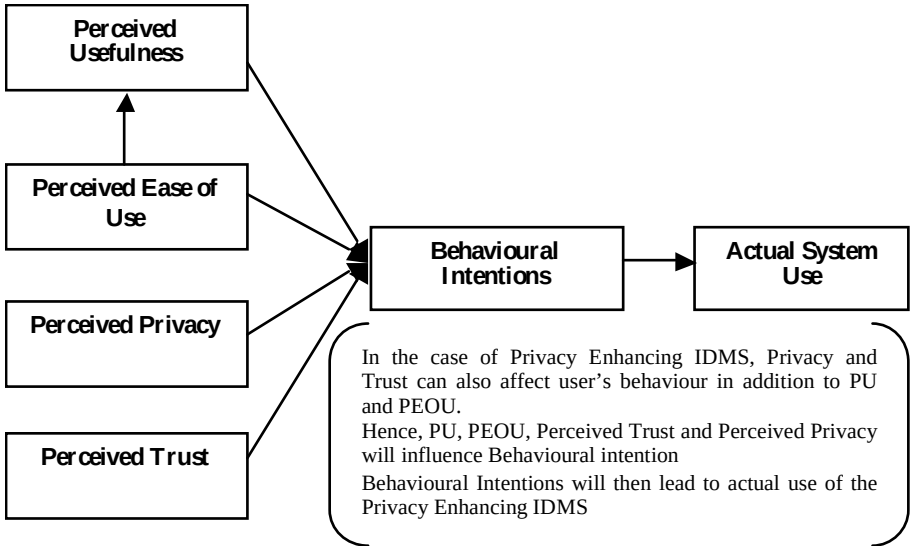


Fig.2. Technology Acceptance Model applied to privacy-enhancing identity management. The diagram shows that users' privacy behaviour is influenced by how easy it is to use the IDMS, and their perceptions on the system's usefulness, privacy and trust considerations. This behaviour then influences the actual system use. *(Adapted from* [4]*).*

instance, the concept of privacy will result in a system having privacy as a default [22]. Similarly, trust considerations will help in overcoming the "dilemma between identity assurance and privacy (OECD, 2009), (Microsoft_Connect, 2010).

FINDINGS & CONCLUSION

This study analysed the concepts of privacy, trust, and the key regulatory and research initiatives on privacy enhancing IDMS. Major frameworks including the Laws of Identity, the Fair Information Practices principles and the Privacy by Design principles were examined. As a result, we found that perceived privacy and perceived trust should be added as constructs to the Technology Acceptance Model, in order to adequately represent privacy-enhancing identity management for the benefit of users and service providers. This also aids in resolving the "Privacy Paradox" and resolving the dilemma between privacy and identity assurance.

The extensive amount of research in this area has led us to the stage, where we now have a fairly good understanding of design principles and best practices, and we also start to have technologies available for development of services and solutions that can empower users, protect their privacy and support fine-grained control of access to resources online. This work is therefore an important contribution to the further development.

One of the remaining issues is to explore how these frameworks and technologies can address privacy and identity management in the physical world. The mechanisms of establishing trust in the physical world are not necessarily the same as those that are used in the digital world online. As it has been phrased “the Internet was built without a way to know who or what you are connecting to” (Cameron, The Laws Of Identity, 2005). Many of the recent initiatives are aimed at establishing an “identity layer” on the Internet. But since physical identity cards, tokens etc. are use in both worlds we need more work to link the usage and achieve “human integration” [1]. Users need to feel equally comfortable consuming services in the physical and digital world.

REFERENCES

[1] K Cameron. (2005) identityblog [Online] http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.

[2] Ann Cavoukian, "The case for privacy-embedded laws of identity in the digital age. ," 2008.

[3] Peter Schaar, "Privacy by Design," Springerlink, April 2010.

[4] F D Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," MIS Quarterly, vol. 13, no. 3, pp. 319-340., 1989.

[5] Marit Hansen, Ari Schwartz, and Alissa Cooper, "Privacy and Identity Management," IEEE Security & Privacy, 2008.

[6] Raffaele Zallone, "The Privacy Paradox or How I Learned to Have Rights that Never Quite Seem to Work," in AAAI Spring Symposium Series, Palo Alto, California, 2010.

[8] David Mason and Charles D Raab, "Privacy, Surveillance, Trust and Regulation: Individual and Collective Dilemmas of Online Privacy Protection," Information, Communication & Society, vol. 5, no. 3, p. 379 — 381, 2002.

[7] Priscilla M. Regan, "Privacy as a Common Good in the Digital World, ," Information, Communication & Society, vol. 5, no. 3, pp. 382-405, 2002.

[9] Roger C Mayer, James H. Davis, and David F Schoorman, "An Integrative Model of Organizational Trust," The Academy of Management Review, vol. 20, no. 3, pp. 709-734, July 1995.

[10] Robert M Morgan and Shelby D Hunt, "The Commitment-Trust Theory of Relationship Marketing," The Journal of Marketing, vol. 58, no. 3, pp. 20-38, July 1994.

[11] Audun Jøsang, John Fabre, Brian Hay, James Dalziel, and Simon Pope, "Trust requirements in identity management," in Australasian workshop on Grid computing and e-research, vol. 44, 2005.

[12] Patricia A. Norberg, Daniel R. Horne, and David A. Horne, "The Privacy Paradox: Personal Information DisclosureIntentions versus Behaviors," The Journal of Consumer Affairs, vol. 41, no. 1, 2007.

[13] Dennis Calton, Peter Graham, and John Reiners, "Resolving the "privacy paradox" Practical Strategies for Government Identity Management Programs," 2008.

[14] Icek Ajzen, "From Intentions to Actions: A Theory of Planned Behavior," in Action Control: From Cognition to Behavior. New York: Springer-Verlag, 1985.

[15] S Dass and S Pal, "Feasibility and Sustainability Model for Identity Management," India, 2009.

[16] Audun Jøsang and Simon Pope, "User Centric Identity Management," in AusCERT Conference, 2005.

[18] Michael D. Birnhack, "The EU Data Protection Directive: An engine of a global regime," Computer Law & Security Report, vol. 20, pp. 508–520, 2008.

[17] OECD. OECD Guidelines on the Prrotection of Privacy and Transborder Flows of Personal Data. [Online].
http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

[19] OECD, The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers, OECD Digital Economy Papers ed.: OECD Publishing, 2009, vol. 160.

[20] Georg Aichholzer and Stefan Strauß, "The Citizens Role in National Electronic identity Management: A Case-study of Austria," in Second international Conference on Advances in Human-Oriented and Personalized Mechanisms, Technologies, and Services, Porto, Portugal, 2009.

[21] PrimeLife, "From H1.3.5: Requirements and concepts for identity management throughout life," 2009.

[22] Ann Cavaokian. (2010, May) Information and Privacy Commision, Ontario. [Online].
http://www.ipc.on.ca/images/Resources/pbd-implement-7found-principles.pdf

[23] Alan F. Westin, "Social and Political Dimensions of Privacy," Journal of Social Issues, vol. 59, no. 2, pp. 431-453, 2003.

[24] Microsoft_Connect. (2010, Mar) Microsoft Connect. [Online]. https://connect.microsoft.com/site1188

[25] Eran Hammer-Lahav. (2007, Oct.) hueniverse. [Online]. http://hueniverse.com/2007/10/beginners-guide-to-oauth-part-i-overview/

[26] P.J Connolly, "OAuth is the 'hottest thing' in identity management," eWeek, vol. 27, no. 9, pp. 12-13, May 2010.

[27] Faye Fangfei Wang and Nathan Griffiths, "Protecting privacy in automated transaction systems: A legal and technological perspective in the European Union," International Review of Law, Computers & Technology, vol. 24, no. 2, pp. 153-162, 2010.

[28] George R Milne and Maria-Eugenia Boza, "Trust and Concern in Consumers' Perceptions of Marketing Information Management Practices," Journal of Interactive Marketing, vol. 13, pp. 5–24., 1999.

Paper 3

KEEPING IDENTITY PRIVATE:

ESTABLISHING TRUST IN THE PHYSICAL AND A DIGITAL WORLD FOR IDENTITY MANAGEMENT SYSTEMS

Joseph K. Adjei and Henning Olesen

Privacy has become a major issue for policy makers. This has been impelled by the rapid development of technologies that facilitate collection, distribution, storage, and manipulation of personal information. This study is an attempt to understand the relationship between individuals' intentions to disclose personal information, their actual personal information disclosure behaviors, and how these can be leveraged to develop privacy-enhancing identity management systems (IDMS) that the users can trust. Legal, regulatory and technological aspects of privacy and technology adoption are also discussed.

Incidences of cyber fraud and abuse of privacy on the Internet can have serious consequences in electronic business and the users' trust in performing online transactions. When security is breached, it endangers users privacy and trust in institutions. Such security breaches have contributed to a growing desire for efficient and cost-effective measures in the design and administration of IDMS.

Several government and business initiatives seek to place the administration and control of identity information directly in the hands of individuals. These initiatives are aimed at curtailing security breaches and abuses of privacy to boost user confidence in online transactions and interactions. IDMS require that individuals be given the right to exercise control over the collection, use, and disclosure of their personal information—their digital personae. Previous researches have proposed the Laws of Identity [1], Fair Information Practice (FIP) principles [2], and Privacy by Design (PbD) [3]. These proposed frameworks and best practices seek to balance an individual's right to privacy with the organization's legitimate need to collect, use, and disclose personal information. Such attempts to give users the latitude to their digital identities are generally referred to as user-centric.

Unfortunately, researchers and developers of user-centric IDMS have mainly focused on making existing IDMS architectures interoperable, while privacy should actually be at the core of the IDMS design. Again, there is the perception that even though individuals advocate

for their privacy, they have little or no reservations in releasing their personal information in social networks (e.g., Facebook). This so-called privacy paradox [4] is what motivates our study. Furthermore, many of the current initiatives are focused on online solutions and services in the digital world, but identity management needs to take into account the differences between users' behavior in the physical and digital worlds. The objective of this article is to understand the major issues involved in the design of privacy-enhancing IDMS and contribute to improved framework and design principles for these.

Identity Management, Privacy, and Trust

The objective is based on the premise that designing a privacy-enhancing technology is not only a technological problem, but theoretical, social, and regulatory dimensions must also be addressed. The research problem is then: "What factors must be considered in designing privacy-enhancing IDMS that address both online and offline identity management issues?" To address the research question, we analyzed the major privacy and data-protection regulations, research initiatives, and privacy-enhancing technologies in light of technology acceptance model (TAM) [5].

Identity and Identity Management

Identity in information systems consists of traits, attributes, and preferences so an individual can access protected resources and receive personalized services. These services could be online, on mobile devices, or face to face [6]. In essence, identity has both physical and digital dimensions. Digital identity is therefore an electronic representation of a real-world entity or an online equivalent of an individual [7]. Traditionally, IDMS are ran by organizations that control all mechanisms for authentication (establishing confidence in an identity claim's truth) and authorization (deciding what an individual should be allowed to do), as well as any behind-the-scene profiling or scoring of individuals [8]. In this study, we adopt the Van Thuan definition of IDMS as consisting of *processes, policies, and technologies used to manage the complete life cycle of user identities across a system and to control the user access to the system resources by associating their rights and restrictions.* [9]

To ensure protection of privacy, security, and provision of trusted services, different variations of IDMS were used throughout history to establish the basis for trade and governance by means of tokens and technologies, seals, coded messages, signatures, and jewelry [10]. There has been a tremendous growth in online government services, business transactions, and social interactions via a single signon (SSO) [10]. Such activities require efficient and effective user identification and authentication, making IDMS very challenging. Clarke posits that identification is ''the association of data with a particular human being'' [11]. Authentication

is a process that results in a person being accepted as authorized to engage in or perform some activity [12]. Lips suggested a shift in focus toward analyses of the wider societal implications of IDMS implementation and the related social design issues [13].

Concepts of Privacy

Privacy refers to the claim or right of individuals to exercise a measure of control over the collection, use, and disclosure of their personal information. Westin described privacy concern as customers' apprehension over the acquisition and use of their personal data [14]. Until recently, identity and privacy were things in which each human being could exercise a reasonable degree of control [15]. With the advent of Internet and high-speed communication technologies, it has become an illusion for the users to assume physical control over the collection and use of private information since data can be mishandled. For example, in many instances, the users have little or no involvement in the dissemination of their details. In essence, mishandled personal information puts individuals' privacy interests at risk. It is for this reason that governments must protect their citizens. Interestingly, many of the present privacy legislations in Europe were drafted on the basis of the Strasburg Convention of 1981 [15]. Therefore, the legislation does not adequately assist in resolving contemporary privacy-intrusion cases.

Furthermore, what constitutes personal information has comparatively widened due to the increased usage of digital media for business and social interactions, e.g., usernames and passwords. Moreover, the concept of privacy has both collective and individual dimensions [16]. Hence, privacy cannot be conceptualized as autonomy from collective norms. This is what informs the debate on whether privacy protection is best approached on the basis that it is a private or a common good [17]. The rights and obligations of individuals in many countries have therefore been weighed against the collective security and public safety goals—particularly in the United States and the United Kingdom [17].

Concepts of Trust

Privacy concern has far-reaching effects on individuals' attitudes toward IDMS. Where there is the concern of vulnerability, people become apprehensive toward systems. According to Oxford Dictionary, trust is the belief that somebody or something is good, sincere, honest, etc., with no intention to harm or trick. There are different research positions on what constitutes trust and the outcomes of trust [18]. In the literature, trust has been defined as the confidence in an exchange partner's reliability and integrity [19]. This confidence provides the basis for the customers to believe in the reliability and integrity of organizations. It is one of the building blocks for information sharing. Milne and Boza [20] and Norberg et al. [21] ex-

amined how privacy concerns are related to trust. They have suggested that increasing trust can mitigate privacy concerns.

In Mayer et al. [18], trust is conceptually distinct from the behaviors that may or may not reflect it. Without a clear distinction between behaviors, the difference between trust and similar constructs is blurred. For instance, Mayer et al. conceptualized trust as the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other party will perform a particular action important to the trustor, irrespective of the ability to monitor or control the other party. Effectively, in a trustworthy relationship, individuals are motivated to share personal information freely with no fear of exploitation. Hence, trust can influence both the positive and negative behaviors of people [22]. Jøsang & Fabre, (2005) observed that the basic ingredients of trust are

- dependence on the trusted party
- reliability of the trusted party
- risk in case the trusted party does not perform as expected.

This implies that trust requirements have a direct correlation with risk exposure. In the study conducted by Mayer et al., three important characteristics of trust were revealed:

- ability
- benevolence
- integrity.

Ability implies competence or perceived expertise. Consistency, fairness, and reliability were used to describe integrity, whereas loyalty, openness, and availability were used to describe benevolence. These trust characteristics are adopted in this study as the constructs of trust and are therefore important factors that must be considered in the design of privacy-enhancing IDMS.

The Privacy Paradox

In many privacy scenarios, commercial interests seek to maximize the value of consumer information. For instance, many Websites that provide useful information make the users register to access the information. Even though individuals may be willing to part with personal information to realize the perceived benefits, many express concern about the violation of their rights and ability to control their personal information. If we had perfect identity, security would not be an issue, just as systems with perfect anonymity will not present any privacy problem. In spite of the complaints, common use of Facebook and Twitter indicates that consumers quite often freely release personal data in their interactions and business transactions [21]. This is referred to as the privacy paradox [15], [21]. The privacy paradox is the relation-

ship between individuals' intentions to disclose personal information and their actual personal information disclosure behaviors. The 2008 IBM survey suggests that individuals see a tradeoff between the increased value of services and the consequent erosion in their privacy [23]. Consumers are on the one hand seeking an online experience that is devoid of fraud, cheap, and more conveniently delivered, yet, on the other hand, there is fear that this could lead to an erosion of users' privacy. In essence, technology has a dual nature: 1) user empowerment and 2) raising security and privacy concerns.

Technology Acceptance Model

Factors affecting technology adoption have been extensively studied in the information systems literature. Morris and Dillon posit that user acceptance is ''the demonstrable willingness within a user group to employ information technology for the tasks it is designed to support'' [24]. Notable research on the adoption and diffusion of technology includes innovation diffusion theory [25], TAM [5], and the unified theory of acceptance and use of technology [26]. In [5], perceived usefulness (PU) and perceived ease of use (PEOU) were theorized to be fundamental determinants of behavioral intentions to accept or reject information technology (Figure 1). PU essentially describes the degree to which a person believes that an innovation will boost their performance [5]. PEOU, on the other hand, describes the degree to which a person believes that adopting an innovation will be free of effort. In effect, users are more likely to adopt systems that are easier to use and offer some benefits since these two factors can affect the behavioral intention to consider using the technology and actually using the innovation. The behavioral intentions are formed on the basis of an individual's attitude, subjective norms, and perceived control of an outcome [27]. PU, PEOU, and behavioral intentions have already been proven to be a reliable means for determining adoption of technology [5], [28]. This study introduces aspects of trust and privacy in the design of privacy-enhancing IDMS. This is based on the premise that users will feel comfortable with systems that protect their privacy and are more likely to release personal information to only trusted third parties—the essence of user centricity [29].

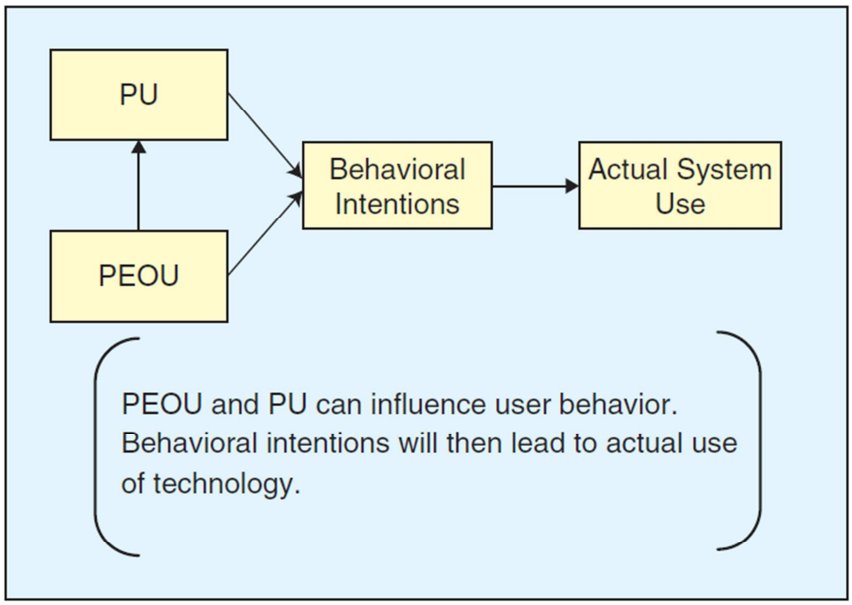


FIGURE 1 The main elements of TAM. (Adapted from [5]).

Frameworks and Initiatives

Regulatory Framework on Privacy

Motivation for good behavior can generally be analyzed based on the risk of data disclosure and regulatory exposure. Regulation in this regard can be categorized as national and international. The FIP principles are a set of such principles developed in the 1970s, which has been adopted by many government agencies, public interest groups, and private companies around the world [8]. The Organization for Economic Cooperation and Development (OECD) issued a set of data-protection guidelines that are an adaptation of FIPs. These guidelines focus on privacy as personal data flows between member countries. It addresses the collection and use of personal data such as names, addresses, and government issued identifiers. The OECD guidelines are very instructive for the design of privacy-enhancing IDMS. The key sections are as follows [30]:

- *Collection Limitation: Limits to the collection of personal data should exist. Personal data should be collected by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject (the individual).*
- *Data Quality: Personal data should be relevant to the purpose for which it is collected and used. It should be accurate, complete, and timely.*
- *Purpose Specification Principle: The purpose for which personal data are collected must be specified no later than at the time of data collection, and its subsequent use must be limited to the fulfillment of those purposes or such others as are not incompatible with the original purpose and as are specified on each occasion of change of purpose.*

- *Use Limitation: Personal information should not be disclosed or otherwise used for other than a specified purpose without the consent of the individual or legal authority.*
- *Security: Reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification, and disclosure should protect personal data.*
- *Openness: The existence of systems containing personal data should be publicly known along with a description of the system's main purposes and uses of the personal data in the system.*
- *Individual Participation: An individual should have the right to obtain confirmation from a data controller, or otherwise, any information relating to them within a reasonable time. The cost of obtaining such information must be reasonable and in a form that is readily intelligible to him.*
- *Accountability: The keepers of personal data should be accountable for complying with the FIPs. These principles are the logical starting point for anyone designing an* IDMS.

There are various country- (or region-)specific laws on privacy that seek to protect privacy. In Europe for instance, many of the privacy and data-protection laws have been brought together as a harmonized European Union (EU) data-protection directive. All EU member states are required to comply. The directive provides the mechanisms to track misuse of personal data and protection against the misapplication of personal data [31]. Unlike the FIPs, breaching legislations and directives can result in prosecution in courts. The major defects of the regulatory framework are twofold. In the first place, as FIPs were implemented long before the World Wide Web and digital age [8], they are inadequate in dealing with modern privacy since acquisition and use of personal information occurs in microseconds and usually with no direct involvement of parties. Secondly, on the Internet, there are no specific border demarcations, making it difficult to enforce country- or region-specific laws on privacy and data protection. This is because culprits might not be nationals of the countries where the incidence occurred (e.g., the WikiLeaks cases). The Copenhagen Privacy Workshop 2011 came up with some recommendations, which were summed up in the Copenhagen Privacy Principles (CPPs) [32]. Some of the key recommendations were the need for a mandatory privacy risk assessment and privacy impact assessment. Another key suggestion was the possible measures taken to enhance privacy protection, which included the right to not be tracked and traced without consent, the introduction of metadata when collecting data to aid data expiration and deletion, and the right to have data deleted upon request (the right to be forgotten).

User-Centric IDMS

The focus on users' quest for power to exercise informational self-determination has resulted in several user-centric and claims-based IDMS initiatives [1], [33], [34]. User-centric IDMS is an approach to give users greater control over their personal information. However, the notion of user centricity does not imply a tradeoff between security and usability but rather a focus on users' privacy and trust. For instance, in their Austrian IDMS study, Aichholzer and Strauß [35] identified equality of access, privacy protection, and user convenience as major factors determining users' acceptance of IDMS. Cameron's seven Laws of Identity [1] have therefore been widely regarded as a guide for providing user-centric IDMS solutions. Generally, the Laws of Identity prescribe the need for consistent user experiences in online transactions, user understanding, user choices and control, and minimum disclosure of user information to only the intended parties.

Identity providers therefore act as trusted third parties to store user accounts and profile information and authenticate users [36]. Service providers, on the other hand, accept assertions or claims about users from the identity providers. Since identity providers do not form a federation in a user-centric IDMS model, they are seen as operating in the interest of users instead of service providers (also called relying parties). A feature in user-centric IDMS, which makes them more privacy enhancing, is the fact that users have the privilege of choosing what information to disclose when dealing with service providers in particular transactions and still satisfy the need to provide certain information for the transaction required [35], [36].

Privacy Research Initiatives

To address the inefficiencies of regulations discussed above, a wide range of industry, academic, and governmental organizations in Europe joined forces in a number of research projects [among these Privacy and Identity Management for Europe (Prime) and Privacy and Identity Management in Europe Throughout Life (PrimeLife)] [33] that have developed working prototypes of privacy-enhancing IDMS. These EU initiatives provide very good frameworks for building privacy-protecting IDMS, although they do not cover the U.S.-specific regulations. Kim Cameron, Microsoft Identity Architect, and Ann Cavoukian, Ontario's Information Privacy Commissioner, have done a lot of research on privacy, which is becoming an industry standard. In her article ''7 Laws of Identity: The Case for Privacy-Embedded Laws in the Digital Age'' [2], Cavoukian offered a unique interpretation of Cameron's Laws of Identity. Cavoukian further proposed seven foundational privacy principles, referred to as PbD principles. Her proposal was based on the notion that innovation, creativity, and competitiveness must be approached from a design-thinking perspective [37]. In a separate study,

Schaar posits that ‘‘PbD is an adjuvant for all kinds of IT systems designated or used for the processing of personal data. It should be a crucial requirement for products and services provided to third parties and individual customers’’ [3]. Table 1 provides a summary of the seven Laws of Identity, the FIPs, and Cavoukian’s PbD. The seven Laws of Identity describe the basis for a unifying identity metasystem that can be applied to identity on the Internet. The identity metasystem is an interoperable architecture for digital identity, which assumes that users will have several digital identities based on multipleunderlying technologies, implementations, and providers [1]. It ensures that not only are individuals in control of their identity but also the organizations will be able to continue to use their existing identity infrastructure investments, choose the identity technology that works best for them, and more easily migrate from old technologies to new technologies without sacrificing interoperability with others [1]. The major informational privacy [14] emanating from digital identities in the identity metasystem are observability and linkability. Observability is the possibility that others, including communicating parties, service providers, eavesdroppers, and third parties,will gain information. Linkability, on the other hand, describes the possibility of linking different data or data sets to an individual for further analysis.

TABLE 1 *Mapping of the Laws of Identity, the FIPs, and PbD.*

Seven Laws of Identity	*FIPs*	*PbD*
1) *User Control and Consent*: Technical identity systems must only reveal information identifying a user with the user’s consent.	Collection limitation	Privacy as a default setting
2) *Minimal Disclosure for a Constrained Use*: The identity metasystem must disclose the least identifying information possible, as this is the most stable, long-term solution.	Data quality	Privacy as a default setting
3) *Justifiable Parties*: IDMS must be designed so that the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.	Purpose specification; use limitation	Privacy as a default setting
4) *Directed Identity*: A universal identity metasystem must support both omnidirectional identifiers for use by public entities and unidirectional identifiers for use by private entities, facilitating discovery and prevent unnecessary release of correlation handles.	Security	End-to-end security. Complete life-cycle protection; proactive and preventive
5) *Pluralism of Operators and Technologies*: A universal identity solution must utilize and enable the interoperation of multiple identity technologies run by multiple identity providers.	Openness	Visibility and transparency—keep it open
6) *Human Integration*: The identity metasystem must define the human user to be a component of the distributed system, integrated through unambiguous human–machine communication mechanisms offering protection against identity attacks.	Individual participation	Privacy enhancing design; full functionality
7) *Consistent Experience Across Contexts*: The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.	Accountability and audit	Visibility and transparency—keep it open

Privacy-Enhancing Technologies

The move to online services offers great promise in terms of both cost reduction and improved user experience. However, the realization of this promise has been severely hampered

by the lack of trust on the Internet specifically, the absence of a practical mechanism for users to obtain and present strong, verified digital identity information online.

In some cases, the information is simply not available in digital form; however, even when it is available, the current set of identity technologies force a tradeoff between the level of identity information assurance that can be achieved and the level of privacy given to users. Further, the users' experience for providing this information are often inconsistent and difficult and sometimes redundant. Digital identity must embrace both being public and private by providing both anonymity and pseudonymity. It always exists in a context, and we expect the context to have the same degree of separation, which we are used to in the natural world, even though space and time no longer serve as insulation. In a user-centric IDMS, the issue of distrust between the user and the relying party is addressed, because the identity provider acts as a trusted third-party broker. This occurs because individuals may have several identity providers, and for that matter, their information may not be stored in one place. The user will naturally trust brokers who can control, whereas the relying parties will not trust a broker if the claims asserted are actually self-vouched by the user [29], [36].

This is what the state-of-the-art technologies and frameworks such as U-Prove, identity mixer (IDEMIX), and open authorization (OAuth) technologies seek to address by managing claims and attributes so that the relying parties are assured that the information is correct before engaging with the user, without necessarily revealing the identity of the user. This approach will still leave the user in control. U-Prove [38], IDEMIX [39], and OAuth [40] enable the use of services with minimum disclosure of personal information and fine-grained delegation of authorization between service providers. Some of their features are summarized in the following.

U-Prove

U-Prove [38] is an advanced cryptographic software designed for electronic transactions and communications to overcome a long-standing dilemma between identity assurance and privacy already mentioned [36], [38]. The technology is part of Microsoft's drive to promote an open identity and access model for individuals, businesses, and governments based on the principles of the identity metasystem [1]. The dilemma is addressed by enabling minimal disclosure of identity information in electronic transactions and communications. To ensure minimum disclosure, the U-Prove agent software acts as an intermediary between Web sites. This allows the users to share data in a manner that will protect their privacy, since they can now choose to share or otherwise. U-Prove includes a mechanism that separates the retrieval of information from trusted third parties releasing this information to the destination site. This

implies that the organization issuing the information is prevented from tracking where or when the information is used. The destination site is similarly prevented from linking users to their activities.

IDEMIX

IDEMIX [39] is an anonymous credential system developed at IBM Research that enables strong authentication and privacy at the same time. Privacy is guaranteed by solving the privacy dilemma and enabling sustainable secondary use of identities over the whole identity life cycle by various partners without trust erosion. IDEMIX follows Ann Cavoukian, a proponent of PbD, that the best way to protect sensitive information is never to reveal it at all. Hence, the desired goal of all privacy-enhancing technologies is to mask sensitive personal information during online transactions and thereby fulfilling the privacy principle of data minimization. Presentation of traditional identity tokens such as passports and ID cards can reveal vital and unwarranted information to third parties by virtue of it being on the token. Credentials are fundamental concepts in IDEMIX implementation. A credential in this case is a means to establish a claimed identity, roles, or attributes about oneself with an entity, typically as part of an access-control request. For instance, an IDEMIX identity card can serve as a credential to establish that a user is above 18 years of age as a requirement to access a gaming site. In essence, by using anonymous credentials, the user can selectively reveal any of the attributes contained in the credential without revealing unnecessary personal information, giving the opportunity for the relying parties to link the identity attributes. IDEMIX works by allowing a computer user who has the appropriate software to obtain an anonymous digital credential or voucher (containing all the information the issuer is ready to reveal) from a trusted third party such as a bank, insurance company, or government agency. When a user later wants to prove to a service provider a statement about her, she employs IDEMIX to securely transform the issued credential. The transformed credential will only contain the subset of the attested information that she is willing to disclose. The user can apply this transformation as many times as she wants, and still none of the credentials can link to each other. As consumers hand over personal details in exchange for downloading music or subscribing to online newsletters, they leave a data trail behind that reveals pieces of information about the size, frequency, and source of their online purchases that can be traced back to the user. IBM's IDEMIX software eliminates the trail by using artificial identity information, known as pseudonyms, to make online transactions anonymous. For example, the software allows the people to purchase books or clothing without revealing their credit card number. It can confirm someone's spending limit without sharing their bank balance or provide proof of age

without disclosing his or her date of birth. ‘‘Unlike other IDMS that transmit parts of a user’s true identity, systems built using IDEMIX software will help protect user privacy by sharing only pseudonyms, so real identity information can never be intercepted or exposed,’’ explains Jan Camenisch of IBM Research, the project lead and head designer (IDEMIX) [41].

OAuth

OAuth [40], [42] is an open standard for authorization, which gives users the ability to grant third-party access to their resources without sharing their passwords [40]. It provides a way to grant limited access (in scope and duration). OAuth allows the users to share their private resources (e.g., photos, videos, contact lists, bank accounts) stored on one site with another site without having to hand out their credentials, typically username and password. The concept of OAuth is based on the valet key metaphor for a car since it only gives third parties a controlled (limited) access to the car [40]. OAuth mimics the valet key metaphor by providing sites with just enough information to accomplish what the user has requested but not allowing third-party sites access to any other user information. Precisely, it only allows the users to hand out to third parties tokens (instead of credentials) to their data hosted by a given service provider. The tokens could be granting a printing service access to photos without sharing username and password. OAuth 2.0, which is the latest version, focuses on client-developer simplicity (not user simplicity) while providing specific authorization flows for Web and desktop applications, mobile phones, and living room devices [40].

Improved Framework and Guidelines

The fact that privacy laws are based on the principles drafted many years ago when the Web did not exist, shows that privacy legislation needs to make a quantum leap to be in line with the realities of today’s real-life operating environment. In cyberspace, there are no clear visual cues about the level of privacy available [16]. Existing privacy legislations and regulations do not adequately deal with the digital identity issues, because laws are country- or region-specific, and the FIPs are not laws. Important privacy considerations exist in relation with data collection, data usage, storage, data minimization, anonymity, pseudonymity, and the extent to which the individuals have control over their personal information. Generally, identity systems that facilitate anonymity and pseudonymity may offer better promise of privacy. In essence, to ensure privacy, risk of vulnerability, the life span of identity information, and the costs of processing, storage and deletion are critical.

Linking identities that do not share the same degree of anonymity or that contain different sets of attributes may allow others to overcome pseudonyms and discover the user’s identity. Questions may arise as to which identity management practices, i.e., data collection, use, and

retention can be subjected to market forces and which of them should be subjected to government interventions. Controlling linkability involves both maintaining separate contexts

so that the observers cannot accumulate sensitive data and being cautious when identity information is requested to keep track of information disclosure [8]. Since much of the literature on privacy-enhancing initiatives aims at introducing technologies with the user in mind, it was apparent that the analysis is carried out in light of TAM. For instance, if privacy must be at the core of the design [37], then obviously the original TAM must be extended to include privacy as a construct. Likewise, to address the dilemma between identity assurance and privacy, trust must be added as a construct. We therefore propose to add perceived privacy and perceived trust as constructs to the original TAM (Figure 2). As shown in the diagram PU, PEOU, perceived trust, and perceived privacy will affect users' behavioral intentions and, in the end, their decision to conveniently use the IDMS. IDMS having privacy-design flaws can generate adverse consequences for consumers, including the risk of identity theft. On the contrary, IDMS can play a privacy-protective role, particularly in the context of social interactions. On the basis of this extended theoretical framework, recommendations for the improved design of privacy-enhancing IDMS can be derived. Table 2 is a summary of the major items, which must be taken into consideration during the design of privacy-enhancing technologies. For instance, the concept of privacy will result in a system having privacy as a default [37]. Similarly, trust considerations will help in overcoming the dilemma between identity assurance and privacy [36], [38].

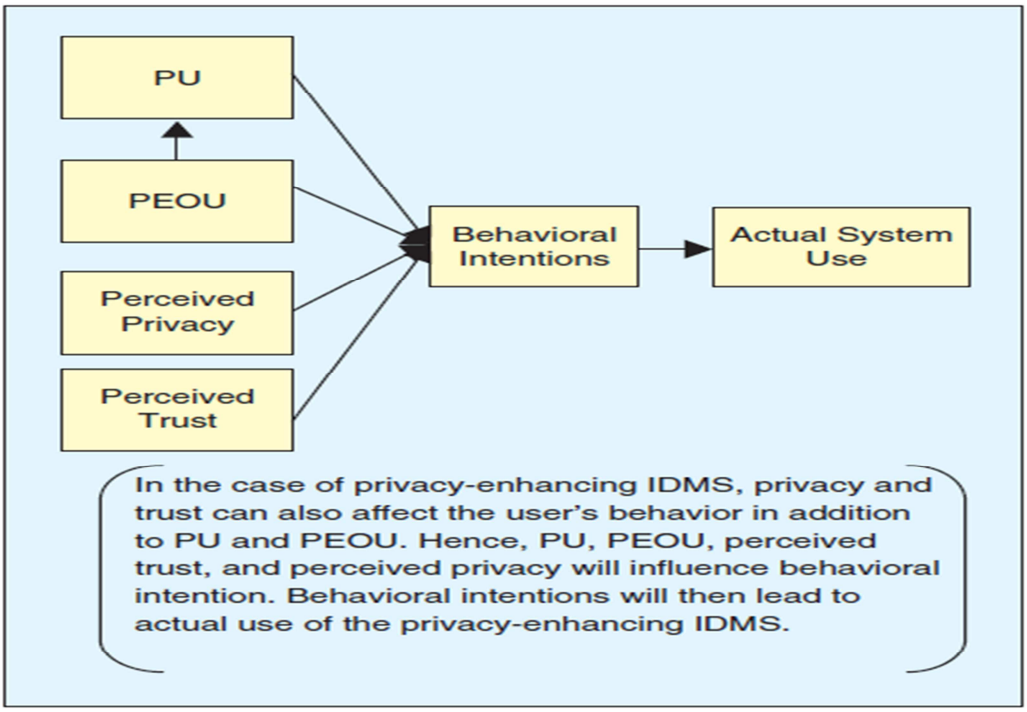


FIGURE 2 TAM applied to privacy-enhancing identity management. The diagram shows that the users' privacy behavior is influenced by how easy it is to use the IDMS and their perceptions on the system's usefulness, privacy, and trust considerations. This behavior then influences the actual system use. (Adapted from [5]).

Design Guidelines for Privacy-Enhancing IDMS Privacy protection has been traditionally based on laws, policies, and regulations with the aim of protecting the individual from large entities such as corporations and governments [43]. Lately, various privacy-enhancing initiatives on a national scale, such as CPPs by European Privacy Association and the White House's National Strategy for Trusted Identities in Cyberspace [44], are aimed at enhancing online choice, efficiency, security, and privacy. These initiatives make provisions for protecting one's privacy from other individuals by addressing issues such as hacking online stalking and voyeurism [45]. On the other hand, there are various industry-driven initiatives such as Microsoft's U-Prove and IBM Research's IDEMIX, which have been greatly influenced by Cameron's Laws of Identity. Overall, governments and policy makers are yearning for the application and compliance with the privacy initiatives. From a design perspective, IDMS developers have been preoccupied with the technical issues by focusing on providing privacy awareness instead of privacy being at the core of design [2], [45]. It is therefore imperative that the design guidelines are proposed to ensure that all the fine-grain issues are considered that will put privacy issues into perspective. Privacy can be perceived from normative, social, and technical perspectives. In [45], the social perspective of privacy focuses on what practices relate to privacy, while the normative aspects are about whether a particular behavior is ethically (or legally) justified. The technical dimension of privacy must therefore focus on how the ethical (or legal) and social understandings can be represented formally and implemented

practically in an operational system [45]. In other words, the designers must address the questions regarding the criminal consequences when individuals' privacy rights are violated. Our proposed guidelines address these issues by looking at these questions, given that the three perspectives of privacy are not mutually exclusive but interdependent. From the social perspective, developers must include features that enhance security and data quality, ease of use, and the capability in offering both online and offline a satisfactory user experience. From the normative perspective, developers must be aware of existing regulatory framework and provide users a level of assurance such that the systems can be trusted and are secure. From the technical perspective, developers must consider the contexts such as offline or online, commercial or informational, and local or cross border. These factors are summarized in Table 2 as PU, PEOU, perceived privacy, and perceived trust.

TABLE 2 *Factors to be considered in the design of privacy-enhancing IDMS.*

Item	*Measurement Criteria*	*Description*
PU	Ease of use, enhanced security, identity fraud prevention, and data quality	Perceived usefulness describes the degree to which a person believes that an innovation will boost their performance.
PEOU	User centricity and universal coverage (online/offline)	PEOU describes the degree to which a person believes that adopting an innovation will be free of effort.
Perceived privacy	Best practices, regulations, and PbD	Application of laws, regulations and the laws of identity.
Perceived trust	Ability	The group of skills, competences, and characteristics that enable a person to have some influence within a domain or context [18].
	Benevolence	The extent to which the trustee is believed to want to do good to the trustor irrespective of profit motives.
	Integrity	Integrity is the perception that the trustee will adhere to a set of principles that the trustor subscribes to.

Privacy laws may be enacted based on technical or social considerations, while social interactions may be altered due to changing laws and technology.

Conclusions

This study analyzed the concepts of privacy, trust, and the key regulatory and research initiatives on privacy enhancing IDMS. Major frameworks including the Laws of Identity, the FIP principles, and the PbD principles were examined. As a result, we found that perceived privacy and trust should be added as constructs to the TAM, to adequately represent privacy-enhancing identity management for the benefit of users and service providers. This aids in resolving the privacy paradox and resolving the dilemma between privacy and identity assurance.

The extensive amount of research in this area has led us to the stage, where we now have a fairly good understanding of design principles and best practices, and we also have technologies available for the development of services and solutions that can empower users, protect their privacy, and support fine-grained control of access to resources online. This article is therefore an important contribution to further development. The existing legal framework is

not sufficient to secure the protection of privacy and has to be improved. The CPP's when implemented will improve and strengthen the existing privacy legislations. Having had a thorough review of privacy-enhancing policies, legal framework, and research and commercial initiatives, it seems to us that underlining the reason driving privacy-enhancing IDMS is to enable the users to prove a predicate of their identity without giving third parties the opportunity to access unwarranted information.

One of the remaining issues is to explore how these frameworks and technologies can address privacy and identity management in the physical world. The mechanisms of establishing trust in the physical world are not necessarily the same as those that are used in the digital world online. As it has been phrased ''the Internet was built without a way to know who or what you are connecting to'' [1]. Many of the recent initiatives are aimed at establishing an identity layer on the Internet. But since physical identity cards and tokens are used in both worlds, we need more work to link usage and achieve human integration [1]. The users need to feel equally comfortable consuming services in the physical and digital world.

Author Information

Joseph K. Adjei (adjei@cmi.aau.dk) obtained his M.Sc. degree in information technology in 2000 from London Southbank University, United Kingdom. He is a Ph.D. student at Aalborg University Copenhagen (AAU-Cph), Denmark. His research focuses on developing better frameworks for implementing privacy-enhancing identity management systems. He is a fellow of the Chartered Association of Certified Accountants (ACCA). His research interests include privacy and user-centric identity management.

Henning Olesen (olesen@cmi.aau.dk) received hisM.Sc. degree in electrical engineering in 1980 and Ph.D. degree in 1982, both from the Technical University of Denmark (DTU) and within the area of optical communications. During 1982–1984, he was a postdoc at DTU and,

in 1984–1995, was a senior research engineer at TFL (Tele Danmark Research) within the field of optoelectronics. During 1996–1999, he did development work in Tele Danmark R&D on digital media, services, and innovation projects and became the leader of Tele Danmark's MediaCenter. During 1999–2008, he was an associate professor at DTU, and since 2008 he has been with the center for communication, media, and information technologies (CMI) at AAU-Cph. He is an associate professor at AAU-Cph, Denmark. He has published more than 100 journal and conference papers and given several invited talks. His research interests in-

clude mobile media and service architectures, user requirements, personalization, and privacy and identity management.

References

[1] K. Cameron, 2005. Identityblog.com. [Online]. Available: http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

[2] A. Cavoukian, ‘‘7 laws of identity: The case for privacy-embedded laws of identity in the digital age,’’ in White Paper, 2008.

[3] P. Schaar, (2010, Apr.). Privacy by Design, [Online]. Available: www.Springerlink.com

[4] D. Calton, P. Graham, and J. Reiners, ‘‘Resolving the ‘privacy paradox’ practical strategies for government identity management programs,’’ White Paper, 2008.

[5] F. D. Davis, ‘‘Perceived usefulness, perceived ease of use, and user acceptance of information technology,’’ MIS Quart., vol. 13, no. 3, pp. 319–340, 1989.

[6] Liberty Alliance Project, (2004, Mar.). Liberty alliance project. [Online]. Available: http://projectliberty.org/liberty/content/download/388/2723/file/Liberty_Government_Business_Benefits.pdf

[7] G. Roussos, D. Peterson, and U. Patel, ‘‘Mobile identity management: An enacted view,’’ Int. J. Electron. Commerce, vol. 8, no. 1, pp. 81–100, 2003. [8] M. Hansen, A. Schwartz, and A. Cooper, ‘‘Privacy and identity management,’’ IEEE Security Privacy, vol. 6, no. 2, pp. 38–45, Mar./Apr. 2008.

[9] D. van Thuan, ‘‘Identity management demystified,’’ Telektronikk, vol. 3, no. 4, pp. 11–18, 2007.

[10] 3G Americas ‘‘Identity management; overview of standards and technologies for mobile and fixed Internet,’’ White Paper, 2009.

[11] R. Clarke, ‘‘Human identification in information systems: Management challenges and public policy issues,’’ Inform. Technol. People, vol. 7, no. 4, pp. 6–37, 1994.

[12] E. Whitley. (2009, Nov.). A new way forward for an effective Identity policy in the UK. Vault [Online]. (3), pp. 4–12. Available: http://www.security-news.tv/fileadmin/images/VAULT/vault_03/TheVault_3_digital.pdf

[13] M. Lips and C. Pang. (2008). Identity management in information age government. Exploring concepts, definitions, approaches and solutions. Res. Rep. Victoria Univ. Wellington, New Zealand. [Online].Available: http://www.e.govt.nz/services/authentication/library/docs/idm-govt-08.pdf

[14] A. F. Westin, ‘‘Social and political dimensions of privacy,’’ J. Social Issues, vol. 59, no. 2, pp. 431–453, 2003.

[15] R. Zallone, ‘‘The privacy paradox or how I learned to have rights that never quite seem to work,’’ in Proc. AAAI Spring Symp. Series, Palo Alto, CA, 2010, pp. 199–202.

[16] P. M. Regan, ‘‘Privacy as a common good in the digital world,’’ Inform. Commun. Soc., vol. 5, no. 3, pp. 382–405, 2002.

[17] D. Mason and C. D. Raab, ‘‘Privacy, surveillance, trust and regulation: individual and collective dilemmas of online privacy protection,’’Inform. Commun. Soc., vol. 5, no. 3, pp. 379–381, 2002.

[18] R. C. Mayer, J. H. Davis, and D. F. Schoorman, ‘‘An integrative model of organizational trust,’’ Acad. Manage. Rev., vol. 20, no. 3, pp. 709–734, July 1995.

[19] R. M. Morgan and S. D. Hunt, ‘‘The commitment-trust theory of relationship marketing,’’ J. Marketing, vol. 58, no. 3, pp. 20–38, July 1994.

[20] G. R. Milne and M.-E. Boza, ‘‘Trust and concern in consumers’ perceptions of marketing information management practices,’’ J. Interact. Marketing, vol. 13, no. 1, pp. 5–24, 1999.

[21] P. A. Norberg, D. R. Horne, and D. A. Horne, ‘‘The privacy paradox: Personal information disclosure intentions versus behaviors,’’J. Consumer Affairs, vol. 41, no. 1, pp. 100–127, 2007.

[22] A. Jøsang, J. Fabre, B. Hay, J. Dalziel, and S. Pope, ‘‘Trust requirements in identity management,’’ in Proc. Australasian Workshop Grid Computing and e-Research, vol. 44, 2005, pp. 99–108.

[23] D. Calton, P. Graham, and J. Reiners. (2008). Resolving the privacy paradox, practical strategies for government identity management programs. [Online]. IBM Global Business Services. Available: http://www-935.ibm.com/services/us/gbs/bus/pdf/gbe03114-

usen_idmgnt.pdf

[24] M. G. Morris and A. Dillon, ‘‘How user perceptions influence software use,’’ IEEE Softw., vol. 14, no. 4, pp. 58–65, July/Aug. 1997.

[25] E. M. Rogers, Diffusion of Innovations, 3rd ed.New York, The Free Press, 1983.

[26] V. Venkatesh and F. D. Davis, ‘‘A theoretical extension of the technology acceptance model: Four longitudinal field studies,’’ Manage.Sci., vol. 46, no. 2, pp. 186–204, 2000.

[27] I. Ajzen, ‘‘From intentions to actions: A theory of planned behavior,’’in Action Control: From Cognition to Behavior, J. Kuhl and J. Beckman,Eds. Heidelberg: Springer-Verlag, 1985, pp. 11–39.

[28] S. Dass and S. Pal, ‘‘Feasibility and sustainability model for identity management,’’ IIMA Research and Publications, India, W.P. No. 2009-12-01, India, 2009.

[29] A. Jøsang and S. Pope, ‘‘User centric identity management,’’ in Proc. AusCERT Conf., 2005, pp. 77–89.

[30] OECD. (2002). OECD guidelines on the protection of privacy and transborder flows of personal data. [Online]. Available: www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

[31] M. D. Birnhack, ‘‘The EU data protection directive: An engine of a global regime,’’ Comput. Law Security Rep., vol. 24, no. 6, pp. 508–520, 2008.

[32] European Privacy Association, (2011, Mar.). The Copenhagen privacy principles [Online]. Available: http://www.cppw.dk/CPP_short_final.pdf

[33] PrimeLife project, ‘‘From H1.3.5: Requirements and concepts for identity management throughout life,’’ EU FP7 PrimeLife Consortium, Heartbeat H1.3.5, Nov. 2009.

[34] FIDIS. (2007, Nov.). Future of identity in the information society. [Online]. Available: http://www.fidis.net/resources/fidis-deliverables/

[35] G. Aichholzer and S. Strauß, ‘‘The citizens role in national electronic identity management: A case-study of Austria,’’ in Proc. 2nd Int. Conf. Advances Human-Oriented and Personalized Mechanisms Technologiesand Services, Porto, Portugal, 2009.

[36] OECD. (2009, June 11). The Role of digital identity management in the internet economy a primer for policy makers. DSTI/ICCP/ REG(2008)10/FINAL, OECD’s Working Party on Information Security

and Privacy. [Online]. Available: http://www.oecd.org/dataoecd/55/48/43091476.pdf

[37] A. Cavoukian. (2010, May). Privacy by design: The 7 foundational principles. [Online]. Available: www.ipc.on.ca/images/Resources/pbd-implement-7found-principles.pdf

[38] Microsoft_Connect. (2010, Mar.). Microsoft U-Prove community technology preview R2. [Online]. Available: https://connect.microsoft.com/site1188

[39] IBM Research. (2010). IDEMIX (identity mixing). [Online]. IBM Research. Available: http://www.zurich.ibm.com/pri/projects/idemix.html

[40] E. Hammer-Lahav. (2007, Oct.). Beginner's guide to OAuth—Part I: Overview. [Online]. Available: http://hueniverse.com/2007/10/beginners-guide-to-oauth-part-i-overview/

[41] IBM Research. (2007). IBM software safeguards consumer identity on the Web [Online]. Available: http://www.zurich.ibm.com/news/07/idemix.html

[42] P. J. Connolly, ''OAuth is the 'hottest thing' in identity management,''eWeek, vol. 27, no. 9, pp. 12–13, May 2010.

[43] L. Lessig, Code: And Other Laws of Cyberspace, Version 2. New York, Basic Books, 2006.

[44] The White House. National strategy for trusted identities in cyberspace:enhancing online choice, efficiency, security, and privacy,Washington. [Online]. Available: www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf 2011.

[45] S. Patil and A. Kobsa, ''Privacy considerations in awareness systems: Designing with privacy in mind,'' in Awareness Systems, Human–Computer Interaction Series, London, Springer-Verlag, 2009, pp. 187–206.

Paper 4

Secondary Uses of Personal Identity Information: Policies, Technologies and Regulatory Framework

Joseph K. ADJEI & Henning OLESEN

Center for Communication, Media and Information Technologies (CMI)

Aalborg University Copenhagen, Denmark

Abstract: Although personal identity information must primarily be used for protecting and promoting the physical needs of individuals, it has also become central to the business models of the digital age due to its use for other secondary purposes, resulting in various innovative identity management (IdM) solutions in OECD countries. Nonetheless, developing countries were still not able to address basic identification challenges such as civil registration, real-time credentials verifications, etc. This paper discusses a means of communicating identity-related concepts to policy-makers, technologists, credential issuers and other stakeholders by addressing core issues relating to secondary use of personal information. The results of a stakeholder workshop in Ghana on secondary use of personal information are presented by stating the core issues and recommendations. We propose the adaptation and application of existing IdM research and experiences from OECD countries to deal with issues involved in using personal information for secondary purposes.

Key words: identity, identity management, personal information, secondary use, trust, privacy.

Technological advancements have paved the way for fast, easy and relatively cheap collection, aggregation and analysis of large volumes of data by third parties, with little or no involvement of the data subject [27] (MALHOTRA, KIM & AGARWAL, 2004; BÉLANGER & CROSSLER, 2011). At the core of these developments is the commoditisation of personal information, which has become a key component of modern business models. Parties in busi-

[27] Data subject is the individual to whom personal data relates.

ness transactions and social interactions usually rely on unique credentials [28] for proofs of identity, which sometimes are unrelated to the primary purpose of the credentials. Such secondary uses of personal information are necessary in various jurisdictions, because the majority of business transactions and social interactions entail various forms of identity verifications and identity assurances. For instance, passports are primarily issued to aid border control, but sometimes might be required by banks or car rental agencies as proof of identity. Incidentally, such personal information usage also presents complex ethical, technological and policy challenges, which usually border on privacy, trust and security. These challenges have played a significant role in preventing access to and expansion of personal identity information (or simply "personal information") uses for secondary purposes.

Research consortiums and technology business organisations in countries within the Organisation for Economic Co-operation and Development (OECD) have developed cutting-edge solutions for addressing both offline and online technological and regulatory issues in identity management systems (IdMS), e.g. U-prove (Microsoft_Connect, 2010), OpenID (RECORDON & REED, 2006), Idemix (IBM_Research, 2010), Touch2id (Evry, 2010), etc. These developments can aid successful or effective uses of personal information for secondary purposes. For instance, businesses can now instantly verify the authenticity of credentials presented by clients, whilst maintaining the privacy of the holder. Government agencies can rely on information in identity databases to offer targeted social services to citizens.

In developing countries identification problems continue to persist, although many different credentials and tokens are issued to citizens, sometimes at a huge cost to the state. In Ghana, for instance, several independent IdMSs have been implemented resulting in the distribution of many forms of credentials. National Identification Cards, Birth and Death Registration, National Health Insurance Cards, Biometric Passports, Biometric Driver's Licences, Biometric Voter's Identity Cards and Tax Identification Numbers (TIN) are some of the widely used credentials.

All the IdM projects have focused on physical verification by the issuer [29] or their agencies in fulfilment of their mandate, with little emphasis on secondary usage by third parties and

[28] Credential is a generic term that can apply to both paper documents like Passports or Birth Certificates, and non-paper based objects such as smartcards and other tokens.

[29] Issuer is an agency that is legally authorised to issue credentials, such as the National Identification Authority or Passport Office.

online or Internet-based transactions. Many of the projects are initiated by government agencies with little private sector participation. Moreover, there is a general lack of interoperability and institutional co-operation contributing to difficulty in verifying the validity of key source documents like birth certificates and identity credentials, multiple registrations, impersonation, etc. Coherent policies, standards and best practices for secondary uses of personal information have therefore become imperative as a result of the growing availability of technologies supporting secondary uses. Addressing the many challenges ultimately requires a national framework for secondary use of personal information that is in the interest of citizens. The issues raised inspired this study to organise a stakeholder workshop to promote national discourse on secondary uses of personal information and their attendant issues.

The objective of this paper is to provide a means of communicating identity-related concepts to policy-makers, technologists, privacy advocates and users. The paper also addresses core issues relating to what constitutes personal identity information and user concerns in relation to secondary uses of personal information. The rest of the paper is structured as follows: The subsequent section discusses the background for this work. We then proceed to a comprehensive literature review discussing primary and secondary uses of personal identity information, the issue of identity, identification and identity management systems, and the major concerns of secondary uses of personal identity information. Subsequently we introduce our methodology for the study. The results from a stakeholder workshop in Ghana and follow-up interviews are presented, followed by a summary and discussion of the findings from the study. We present our conclusions in the final section, making a case for further studies in connection with commercialisation of personal identity information.

Background

Research, development and implementation of identity management systems in OECD countries have progressively gone through many stages, and various models have emerged. Currently, IdMS discussions in OECD countries have moved beyond issues in relation to civil registration coverage of births, silo and federated IdM models to user-centric IdM, where many of the research efforts are focused on identity assurance (EnCoRe, 2012; CROSBY, 2008). Moreover, many of the issues in connection with offline credential presentation and verification have been largely addressed, leading to more emphasis on electronic identity management systems with attribute-based credentials for enhancing privacy and anonymity as the research focus. Several pilot and real life solutions have been successfully tested (CAMENISCH, *et al*., 2011).

On the contrary, many developing countries have still not been able to deal with fundamental identification challenges, and undue emphasis is still on primary usage of tokens by credential issuers and on physical verification, with little room for identity assurance and real-time verification by third parties. Some of the identification challenges can be traced to the reliability of source documents like birth and death register. In Ghana, for instance, the birth registration coverage is 71% according to WHO 2012 Health Statistics Report (WHO, 2012). This situation hinders the reliability of identity tokens for secondary uses by businesses and government agencies.

Existing IdM initiatives in Ghana are heterogeneous and independently managed with little involvement of other government agencies and the private sector. The various identification databases are all in silos and used primarily by the credential issuers as a means of fulfilling their main objective – e.g. voters' identity card is for electoral purposes. If a citizen's status changes (e.g. name change due to marriage), or the citizen changes address, the necessary changes have to be made with all the credential issuers separately. Moreover, Internet applications of such credentials have not been a priority, thereby all the credentials are mainly for physical verifications. For instance, if a credential is presented for services, the service providers have no formal means of verifying its authenticity in real-time. There are opportunities for application developers to collaborate with credential issuers to develop verification and authentication systems for business. One such scenario is a local business that has developed credential verification application for financial institutions based on the voter register. The major challenge in this regard is lack of clear policies on secondary uses of personal information.

Literature review

An important aspect of the study has been to review IdM-related publications in research journals, and IdMS research and development in OECD countries. The key research works studied were: OECD Digital Economy Papers on identity management, European Union research projects on Future of IDentity in the Information Society (FIDIS) (FIDIS, 2007), Privacy and Identity Management in Europe for Life (PrimeLife), and Attribute Based Credentials for Trust (ABC4Trust [30]) (CAMENISCH *et al.*, 2011); the Kantara Initiative (WILTON, 2008); United Kingdom based research project on Ensuring Consent and Revocation (EnCoRe, 2012) and the US government's National Strategy for Trusted Identities in Cyberspace

[30] http://www.abc4trust.eu/

(NSTIC, 2011). Our study also draws on key IdM and privacy-related articles from *MIS Quarterly* (BÉLANGER & CROSSLER, 2011; PAVLOU, 2011), The Seven Laws of Identity (CAMERON, 2005), and Privacy by Design (CAVOUKIAN, 2008). The authors also listened to and watched various podcasts on U-Prove (Microsoft_Connect, 2010), and Idemix (IBM_Research, 2010) to understand the state-of-the-art in privacy-preserving identity management systems. Unfortunately, there were not many IdMS-related research articles from developing countries.

Identity, identification and identity management

The issue of identity has been widely researched from the perspective of technical scientists, psychologists, sociologists, etc. From a mathematical perspective, Leibnitz defined identity on the basis of whether two things can be distinguished from each other (WILTON, 2008; FELDMAN, 1970). He postulated that two objects sharing similar characteristics like shape, extent, position in time and space, could be deemed to have or share the relationship of identity (FELDMAN, 1970). Likewise, in our day-to-day physical interactions and on the Internet, we leave our footprint in the form of pieces of information about ourselves, which accrete in various ways as we interact online. A person's identity is regarded as a reflection of those things, which are generally known about them by the people with whom they interact (WILTON, 2008). Identity is therefore a part of a chain of events from enrolment and credential issue through to credential presentation and hence a process, rather than a state.

Identification on the other hand is the process of linking information with a particular person, thus the action of being identified (CROMPTON, 2004). If identification is a process, then the integrity of the identification process and its usefulness will depend on the following factors: the reliability of the registration processes, verification and enrolment; how difficult it is to duplicate or alter credentials; and the difficulty in verifying the link between the credentials themselves and the person presenting them. To meet such identification criteria, an efficient system for managing identity will be necessary. Identity management therefore consists of the processes and all underlying technologies for the creation, management and usage of identities and their attributes. In effect, identity management unduly focuses on credential issuers and identity service providers with its implication on trust and misinterpretation of secrecy as a means of privacy protection.

Measures aimed at working towards user satisfaction lead to more focus on identity assurance. Identity assurance is a consumer/user led concept that enables data subjects to prove or provide informational representation during a chain of events that can define who they are

without the need for them being physically present (CROSBY, 2008). Identity assurance must be a key element in identity management since it offers mutual benefits to identity service providers and to citizens. An identity assurance scheme can address issues such as the amount and type of data stored and the degree to which this information is shared.

Personal identity information

Personal information has become central to the business models of the digital age; to the management of government and state institutions; and to people's everyday lives and relationships. Business organizations sometimes apply strategies aimed at personalising service delivery to customers by focusing on customer preferences in order to offer specialised services (ALATALO & SIPONEN, 2001). Such practices could offer customers convenience, efficiency and personalisation, which can contribute to repeat of purchases. This inherently requires collection of pieces of customers' personal data or attributes. Among others, this is one reason why there is the need to take a closer look at what constitutes personal information (ANDRADE, KALTCHEVA & WEITZ, 2002).

Personal information is any information that specifically identifies an individual (e.g. name, telephone number, e-mail address, or account number), or their location or activities, such as information about his or her use of a website, when directly linked to personally identifiable information. In his Onion Model (WILTON, 2008), Wilton uses the layers of an onion as an illustration to categorise personal information into three layers – the core, inner layer and the outer layer. Information that can uniquely identify an individual and does not change over time, (e.g. name, date of birth) was placed at the core. Information at the core is known as a Basic Identifier Set (WILTON, 2008). The inner layer consists of information that is capable of being used for identification but susceptible to change over time, such as address, height, etc. The outer layer consists of information that cannot uniquely identify a person, except when combined with some other information or aggregated overtime, such as a person's transaction history and sector specific information like blood group and health status. In effect, personal information is any information describing a natural person or information that describes an identifiable individual (TRUBOW, 1992)

Primary and secondary uses of personal information

Information must generally be used for the purpose of protecting, promoting, or meeting the physical needs of an individual or to enable that individual to participate in social interactions or benefit from services. Such information usages are regarded as the primary purposes of

collecting personal information. For instance, the primary purpose of a Voter ID card is for an individual to vote in an election and that of a passport is to facilitate border control. Many of the data protection regulations mandate that personal information gathered for one purpose may not be used for any other purpose without the specific, informed consent of the data subject (TRUBOW, 1992). However, in order to conduct business such as opening a bank account, banks sometimes require tokens like a passport as a proof of identity. Such a requirement by the bank is secondary to the original intention of passports and voter IDs.

Culnan conceptualised secondary uses of personal information as having two dimensions: (1) The information processing activity (acquisition, use, or transfer) and (2) The relationship between the consumer and the firm utilizing the information (existing customer or prospect) (CULNAN, 1993). Secondary use of personal information therefore implies collection and storage of information for purposes other than originally intended by the issuer of the credential, whether legitimate or otherwise. Access to and use of personal information can in principle pose a number of complex challenges. In effect, for secondary use of personal information to be legitimate, there must be an "implied social contract" (tacit or explicit consent by service provides to protect the interest of data subjects) between service providers and users (MILNE, 1993). Where there is a perception of breach of such confidentiality, it affects the trusting relationship that should exist between service providers and data subjects (SOLOVE, 2006). Given that technological developments make such breaches difficult to notice, secondary use of personal information poses technological, policy and regulatory concerns in relation with the ability to collect, store, aggregate, link, and transmit personal information for legitimate purposes. Such challenges have generally been researched in information systems under information privacy.

Privacy, information privacy and privacy concerns

Privacy is a topic, which has been studied in many different ways due to its many dimensions (SMITH, MILBERG & BURKE, 1996). It has been described as a condition or a state in which an individual can be more or less inaccessible to others, either on the spatial, psychological or informational plane (WHITLEY & KANELLOPOULOU, 2010). From psychology literature, WESTIN (1967) described privacy as the ability of individuals to control the terms under which personal information is acquired and used. From a sociological viewpoint, privacy has been defined as individuals' ability to independently dispose of their roles according to their right of self-determination, and then to have confidence that third parties respect the intended separation of their roles (BISKUP & BRÜGGEMANN, 1988). Defining privacy as an individual's personal space, CLARKE (1999) categorized personal space into four dimensions

– privacy of the person (concerned with the integrity of the Individual's body), privacy of personal behaviour, personal communications, and privacy of personal data. Recent research has merged personal communication and data privacy into what is referred to as information privacy, due to the increased digitalization of information and communications (BÉLANGER & CROSSLER, 2011; PAVLOU, 2011). Hence, information privacy refers to the claims of individuals that their personal data should generally not be available to others, and that, where data are possessed by another party, the individual must be able to exercise a substantial degree of control over the data and their use (BÉLANGER & CROSSLER, 2011).

Information privacy concerns are related to factors affecting a person's willingness to render personal information (DINEV & PAUL, 2006), engage in online transaction activity (PAVLOU, LIANG & XUE, 2007), and the attitude towards government regulation (MILBERG *et al*., 2002). Although individuals express privacy concerns, many are willing to trade-in their privacy for convenience. This so-called privacy paradox (NORBERG, HORNE & HORNE, 2007; ZALLONE, 2010; ADJEI & OLESEN, 2011) also reaffirms the need for a more measured treatment of personal information. Thus, information privacy is not about secrecy, which is an intentional concealment of information and (or) a disposition toward the sharing of potentially inaccurate information (TRUBOW, 1992). OECD guidelines (OECD, 1980), and other national data protection laws address various aspects of information privacy concerns, such as; (1) The existence of record systems cannot be kept secret; (2) an individual must be able to "find out what information about him is in a record and how it is used"; and (3) an individual must be able to "correct or amend a record of personally identifiable information (SOLOVE, 2006).

BÉLANGER & CROSSLER (2011) observed that development of privacy tools and technologies is usually done in isolation of the actual users and for that matter their input are not reflected in the systems design. The research approach adopted in this study is to address such concerns and to ensure active user involvement in secondary uses of their personal information.

Figure 1 – Privacy and dimensions of privacy

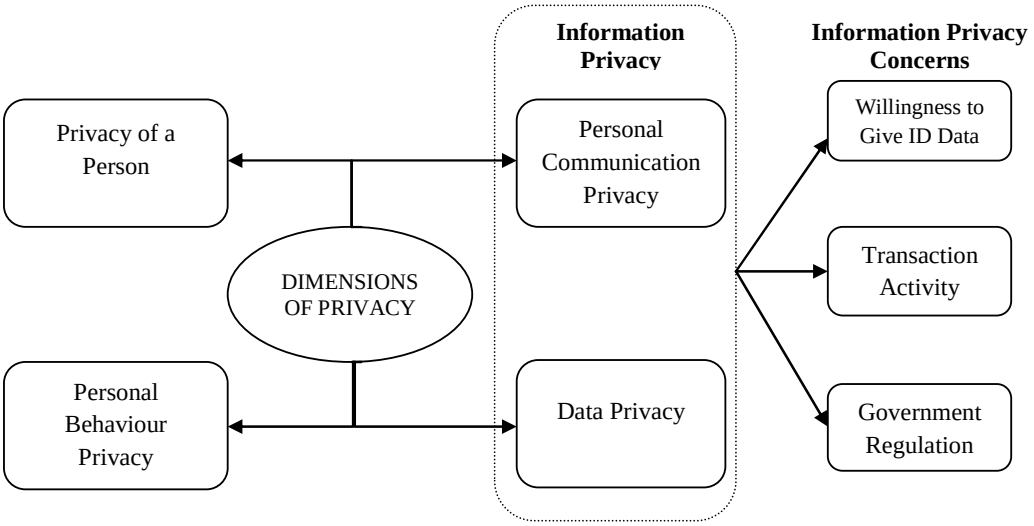


Figure 1 outlines the dimensions of privacy. Information privacy is related to personal communication privacy and data privacy. Major sources of concern are during data collection, data processing and data dissemination. Information privacy concerns affect individuals' willingness to provide information, their transaction activities and responses to government regulations.

Stakeholder workshop and interviews

This study adopted a qualitative methodological approach for data collection (YIN, 2009) resulting in a review of literature on the state-of-art on identity management, privacy issues in secondary use of personal information. The Interpretative Phenomenological Analysis (SMITH, 2004) approach was applied in the data analysis due to its reliability with respect to audio-visual contents, which is very common in focus group and workshop discussions. The issue of concern and for that matter the subject of the study was to find out what needs to be done in order to trigger successful or effective secondary uses of personal information within the context of an economy.

Stakeholder workshop

A stakeholder workshop was organised in Ghana on January 16, 2012, at Ghana Telecom University College (GTUC) in Accra. 75 participants were offered the opportunity to discuss a number of issues and listen to presentations highlighting issues concerning secondary uses of personal information. Letters were written to all the participants, and detailing the theme, agenda and activities for the day. The participants were made up of senior officials from national institutions involved in the collection and storage of personal information, such as Reg-

istrar of Births & Death, The Passport Office, Driver and Vehicle Licensing Agency (DVLA), National Identification Authority (NIA), National Health Insurance Authority (NHIA), Electoral Commission (EC), Ghana Revenue Authority. Also represented were senior officials of the major financial institutions, biometric and identity-related businesses, academic institutions, the media, non-governmental organisations involved in civil right advocacy, and the general public.

Ghana was selected as the research setting because the challenges faced by the economy with respect to identification and secondary uses of personal information are similar to those of other developing countries. Notable challenges include unreliable civil registration systems, electoral issues due to unreliable voters register, lack of identity management systems interoperability, etc. The workshop began with a statement from the Minister of Communication and a keynote address by the President of GTUC, who chaired the event. To inform discussions participants were given background information and copies of the discussion questions during a presentation on privacy and identity management. The presentation highlighted the key concepts on identity management, including major policy, technological and regulatory issues and related IdMS research and practices in OECD countries. This was followed by another presentation on existing secondary uses of personal information for identity verification by financial institutions.

After the presentations participants shared their observations on the topic during the discussion session. Participants were also made to discuss the issues raised and share their experiences and their reservations. Where a particular issue or questions were sector-specific, the agencies concerned were given the opportunity to respond to such questions. Some of the discussion questions were:

What are the potential benefits and risks regarding the secondary use of personal information?

Who has the right to access personal information held by government agencies and for what purposes?

What are the evolving public trust issues with respect to secondary use of personal information?

Do citizens have the right to put constraints on the use of their personal information?

What problems may develop as innovative technologies enhance the ability and ease of widespread personal data sharing for a secondary purpose and commercial uses?

What can be done to address issues arising from inappropriate use and/or exploitation of personal information?

What regulations, legislation, and/or policies and procedures are needed to address these issues?

Interviews

A series of expert and stakeholder interviews were conducted after the workshop to offer stakeholders the opportunity to elaborate on some of the concerns raised by participants. It also offered interviewees the opportunity to clarify some of the points raised during the workshop and to solicit for further information. Interviewees included the officials of identity issuers, policy makers, journalists, private businesses involved in identity verification, and identity card manufacturers.

Transcription and coding

Transcripts of the workshop discussions and the interviews, in the form of audio-visual recordings, interview notes and summary of the discussion session were produced by the authors. The transcription mainly focused on speeches and statements made rather than who said what. This was meant to maintain speaker anonymity. No attempt was made either to identify speech patterns, since that was not the focus of our research. Each of the transcripts was coded on the basis of the introductory background of the various speakers, since each of the participants and interviewees were told to introduce themselves before speaking. This served as a basis for coding and sub-categorisation of the transcript. This style of coding and categorisation aided to consolidate the transcript into analytically distinct segments that could be examined together both within and between groups that covered the same concept (SMITH, 2004; WHITLEY & KANELLOPOULOU, 2010). For instance, statements like "Sorting out accurate birth register can reduce multiple registration", were felt to convey the same ideas as "many people present fraudulent birth certificate for IdMS enrolment". Hence, these two sets of codes were merged.

Results from the workshop and interviews

The organisation of the workshop, the presentations, application demonstrations, and questions and responses, prompted a lively discussion of the key issues, the available opportunities for secondary uses, and the major challenges. The analysis was also based on the major themes from the literature involving constant search through the codes and categories for contradictory and distinct claims and statements from the transcript (WHITLEY & KANELLOPOULOU, 2010).

The workshop enumerated many important issues associated with secondary uses of personal information. The issues were discussed from user, national and business perspectives. However there were areas where there existed commonality of opinions among participants. For instance, many of the participants were of the opinion that "organisations that make a conscious effort to maintain customer's privacy will in return gain customer loyalty". Highlights of the discussion are summarised in the following:

User perspective

From the user perspective, privacy and security of personal information, risk and cost associated with privacy abuses, government intervention policies and programs were of major concern. As an example, there are instances where "a person will go to a bank to withdraw remittances only to find out to their amazement that another person had already withdrawn the funds with that individual's personal details and sometimes fraudulent credentials". The panel discussed privacy implications of a real life scenario, where an identity issuer has authorised a private entity to operate a system for financial institutions to verify the authenticity of credentials, presented by customers. The key challenges to real time electronic information exchange were cost of bandwidth and power fluctuation, which are common in developing countries. Wilton's Onion model of Identity (WILTON, 2008) was also used to discuss, how personal information can be segregated to avoid linkability. It was observed that for users' interest to be served there was the need for emphasis on identity assurance (CROSBY, 2008; WHITLEY & KANELLOPOULOU, 2010)

Business perspective

Major discussion topics included the growing commercialization of personal information where there were several varied opinions. It became apparent that efforts should be made by government agencies to promote effective secondary uses. Panellists observed that there were not many opportunities for secondary uses in Ghana, a situation that is common in many developing countries, and hence the need for creation of a taxonomy of secondary uses of personal information. Two industry viewpoints provoked dialogue, one from the credential issuers, who think that third party verification is not their core business, and a second from the financial institutions, who need such verification to conduct transactions. Tables 1, 2 and 3 outline business, the key roles and responsibilities.

National perspective

The panel discussed the growing use of IdMS for national security, public health, social security, child protection and payment processing. These can only be realised if policy makers and

credential issuers will see personal information not as matter of secrecy but something that, if well managed, can facilitate business transactions and a knowledge economy. Options for adaptation of various OECD research initiatives were discussed including roles and responsibilities of key stakeholders as shown in tables 1, 2 and 3. For instance, the rules for obtaining user consent secondary uses, addressing civil registration issues, etc. There were diverse opinions regarding the most effective and practical approaches to accomplish this, and hence this is a subject for further discussion.

Table 1 – Typical secondary use scenario:
key stakeholders, their interests and responsibilities

Typical Transactions	**Businesses**	**Consumers**	**Identity Issuer**
Online transactions	Business need information on customers and their transaction history	Consumers would like to apply for jobs or make online payment and to ensure privacy protection	Must ensure that credentials held by the right person
Transaction Negotiation	Businesses want prior knowledge of customer preferences.	Consumers would like to know if the seller or the transaction is genuine.	Must ensure real-time credential verification.
Identity Verification	Businesses want proof that customers are legitimate.	Customers need assurance that their privacy is not abused	Enforce minimum disclosure and data security policies
Payment Confirmation	Businesses want assurance that customers are credit worthy	Customers need a proof of total cost to avoid any hidden charges.	Would like to issue credentials that are easy to use
Payment Assurance	Businesses want assurance that customers will pay on due date.	Desires protection against disclosure of payment details and unauthorised deductions	Must ensure that systems are secure from abuse.
Order Fulfilment/ Delivery	Businesses need protection against customers' unjustified cancellation of order.	Customers would like to ensure that goods and services are delivered.	Must ensure that credential information is reliable.

Major findings and discussion

The discussion revealed the need for a paradigm shift with respect to ownership and control of personal information. The "identity" an individual seeks to assert is not their physical being as such, but rather an informational representation of the chain of life events that is defined by who they are. The particular events of relevance depend on with whom the individual is dealing and will lead to different entitlements. In that regard, attention must be focused on access to and control of personal information rather than data ownership. Focusing on data access and controls will ensure that appropriate policies for secondary uses of personal information

will be developed since focusing on data ownership diverts attention from needed policies and practices. The workshop therefore recommended focus on data access, control policies and practices as the best approaches to risk management and mitigation for secondary use of personal information.

Table 2 provides a summary of some of the key recommendations.

Table 2 – Recommendations for secondary uses of personal information

Issues discussed	**Recommendation**
Policy on secondary uses	Implement transparent policies and practices for secondary uses of personal information, taking advantage of available research and technologies.
Access to personal information	Focus on data access and control policies and practices for secondary use of data and not data ownership or secrecy.
Trusted identities	Ensure reliable civil registration.
Benefits and challenges associated with secondary use of information	Increase public education on benefits of secondary use of personal information.
Available secondary uses	Create a taxonomy of secondary uses of personal information and clarify its societal, public policy, legal, and technical implications

Privacy and trust emerged as two major issues; firstly, lack of understanding and inability to differentiate privacy from secrecy; and secondly, inadequacy of safeguard procedures that address user concerns in relation to secondary uses of personal information. In essence, citizens would like to be able to assert their identity with ease and confidence and hence they need such assurances (CROSBY, 2008). The workshop observed that lack of clear regulations (e.g. uses of data obtained via coerced or compelled consent) could result in the erosion of public trust. A taxonomy for identifying possible secondary uses of personal information is therefore required in order to clarify societal, public policy, legal and technical issues arising from secondary use of personal information.

Policy considerations

"As long as we persist with a 17th century notion of national sovereignty, an 18th century judiciary and 19th century law enforcement, the 21st century will belong to organised crime." (Jeffrey Robinson [31])

[31] Jeffrey Robinson: writer on money laundering and organized crime.

Addressing the issues raised requires clearly defined policy initiatives. The following section outlines requirements for appropriate policies to provide high-level guidance for secondary uses of personal information, user empowerment, security, and privacy protection.

Interoperability

Policy issues in relation to IdMS interoperability have legal, business process and technical implications. The challenges are for credential issuers and service providers to articulate clear sets of policies containing a common set of elements, to enable comparison of those policies across organisations, to highlight areas of compatibility and to facilitate policy interoperability. At the legal level, there is the need for regulatory interoperability among various credential issuers in order to minimise regulatory complexities (OECD, 2011).

Information privacy and user empowerment

Many of the digital IdM solutions and privacy related principles like user control and consent, anonymity, (un)linkability, minimum disclosure, etc, implicitly assume a certain level of user literacy. This is not always the case for all users (CAMERON, 2005; OECD, 1980). Public education and awareness programs will play a major role in empowering users and fostering trust.

Security and trust

There is a need for the development of consistent policies to ensure availability, confidentiality and integrity of personal identity data stored and exchanged since these are where user concerns emanates from. Inherent challenges in this regard are the constant availability of the systems and accuracy. Greater transparency in the enrolment and system use will increase citizens' trust in institutions.

Table 3 summarizes the identified responsibilities of the various stakeholders in order to promote the secondary use of personal information.

Table 3 – Stakeholders responsibilities in promoting secondary use of personal information

Principles and guidelines	**Credential issuers**	**Service providers**	**Policy makers**
The Laws of Identity & Privacy by Design (PbD) Guidelines, etc.	Review existing IdMSs to ensure trusted identities	Develop easy to use privacy enhancing applications	Privacy audit of existing mainstream IdMS
Privacy Research Initiatives	Adopt and adapt attribute based privacy enhancing credentials	Develop minimum disclosure applications	Empower users by promoting awareness programmes
OECD Guidelines and	Implementation of in-	Focus on PbD &	Review policies to en-

Data protection laws	teroperability policies	Training	sure process interoperability
Institutional Specific Laws	Identify conflicting areas	Report conflicting laws	Review laws to ensure legal interoperability

Conclusion and further research

Central to effective uses of personal information is an efficient civic registration system, a regulatory framework that encourages institutional collaboration, clear policies and guidelines that provide assurance of citizens' privacy and cost effective application systems. This is what the paper attempted to highlight by using the stakeholder approach and is considered its major achievement. The study has also helped to raise awareness of current technological developments and in IdMS and how developing countries can adapt and apply them. This call has been guided by the fact that application of Digital identity management is a process, rather than a state, the integrity of which depends on: how reliable were the initial processes of registration, verification and enrolment, and how hard is it to duplicate or alter the credentials used? (WILTON, 2008).

Moreover, the use of the stakeholder workshop was as an attempt to bring together users and researchers, public and private sector organizations. It is a key methodological contribution and also a response to BÉLANGER & CROSSLER's (2011) call for closer collaboration between researchers, developers and users to ensure effective uses of privacy enhancing identity management systems.

Like many qualitative research methodologies a key limitation of our study is its lack of empirical testing of the claims compared to quantitative research. Also given that certain societal dynamics are peculiar to different countries, care must be taken in generalizing the findings from our study to other countries.

A follow-up stakeholder workshop that combines focus group discussions to recommend practical solutions for secondary uses of personal information for commercial purposes is planned in the last quarter of 2012.

References

ADJEI, J. K. & OLESEN, H. (2011): "Keeping Identity Private", *Vehicular Technology Magazine, IEEE*, 6(3), 70-79.

ALATALO, T. & SIPONEN, M. T. (2001): "Addressing the personalization paradox in the development of electronic commerce systems", EBusiness Research Forum (eBRF), Tampere, Finland.

ANDRADE, E. B., KALTCHEVA, V. & WEITZ, B. (2002): "Advances in Consumer Research", *Self-disclosure on the Web: the impact of privacy policy, reward, and company reputation*, 29(1), 350-353.

BÉLANGER, F. & CROSSLER, R. E. (2011, December): "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems", *MIS Quarterly* 35(4), 1017-1041.

BISKUP, J. & BRÜGGEMANN, H. H. (1988): "The Personal Model of Data: Towards a Privacy-Oriented Information System", *Computers & Security*, 7, 575-597.

CAMENISCH, J., KRONTIRIS, I., LEHMANN, A., NEVEN, G., PAQUIN, C., RANNENBERG, K. & ZWINGELBERG, H. (2011): "Architecture for Attribute-based Credential Technologies – Version 1", ABC4Trust.

CAMERON, K. (2005): "The Laws of Identity", from identityblog http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.

CAVOUKIAN, A. (2008): The case for privacy-embedded laws of identity in the digital age, Technical report.

CLARKE, R. (1999, February). "Internet privacy concerns confirm the case for intervention", *Communications of the ACM*, 42(2), 60-67.

CROMPTON, M. (2004): "Proof of ID Required? Getting Identity Management Right", Australian IT Security Forum.

CROSBY, S. J. (2008, March): "Challenges and Opportunities in Identity Assurance. From HM Treasury".

http://www.hm-treasury.gov.uk/media/6/7/identity_assurance060308.pdf

CULNAN, M. J. (1993): " 'How Did They Get My Name?': An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use", *MIS Quarterly*, 17(3), 341-363.

DINEV, T. & PAUL, H. (2006): "Privacy Concerns and Levels of Information Exchange: An Empirical Investigation of Intended e-Services Use", *e-Service Journal*, 4(3), 25-60.

EnCoRe - Ensuring Consent and Revocation (2012). http://www.encore-project.info

EVRY, C. (2010): "Proof-of-age scheme prepares to expand across Wiltshire", *Wiltshire Times*.

http://www.wiltshiretimes.co.uk/news/inyourtown/wiltshire/8239556.Proof_of_age_scheme_prepares_to_expand_across_Wiltshire/

FELDMAN, F. (1970): "Leibniz and 'Leibniz' Law' ", *The Philosophical Review*, 79(4), 510-522.

FIDIS. (2007): "Future of Identity in the Information Society", Deliverable-Report. D13.6: Privacy modelling and identity.

IBM_Research (2010): "IDEMIX (Identity mixing) Project Overview". http://www.zurich.ibm.com/pri/projects/idemix.html (retrieved 2012, 28th February

MALHOTRA, N. K., KIM, S. S. & AGARWAL, J. (2004): "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model", *Information Systems Research*, 15(4), 336-355.

Microsoft_Connect (2010): "Microsoft U-Prove Community Technology Preview R2", Microsoft Connect. https://connect.microsoft.com/site1188

MILNE, G. R. (1993): "Direct Mail Privacy-Efficiency Trade-Offs within an Implied Social Contract Framework", *Journal of Public Policy & Marketing*, 12(2), 206-215.

NORBERG, P. A., HORNE, D. R. & HORNE, D. A. (2007): "The Privacy Paradox: Personal Information DisclosureIntentions versus Behaviors", *The Journal of Consumer Affairs*, 41(1), 100-126.

NSTIC (2011): "National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy April 2011", Washington: The White House. http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf (retrieved June 28, 2012)

OECD

- (1980): "From Guidelines on the Protection of Privacy and Transborder Flows of Personal Data". http://www.oecd.org

- (2011): "From Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy - Guidance for Government Policy Makers". http://dx.doi.org/10.1787/5kg1zqsm3pns-en

PAVLOU, P. A. (2011): "State of the Information Privacy Literature: Where are we now and whee should we go?" *MIS Quarterly*, 35(4), 977-988.

PAVLOU, P. A., LIANG, H. & XUE, Y. (2007): "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective", *MIS Quarterly*, 31(1), 105-136.

RECORDON, D. & REED, D. (2006): "OpenID 2.0: a Platform for User-centric Identity Management", Second ACM workshop on Digital identity management (DIM'06) (pp. 11-16), New York, USA: ACM.

SMITH, H. J., MILBERG, S. & BURKE, S. (1996): "Information privacy: Measuring individuals' concerns about organizational practices", *MIS Quarterly*, 20(2), 167-196.

SMITH, J. A. (2004): "Reflecting on the development of interpretative phenomenological analysis and its contribution to qualitative research in psychology", *Qualitative Research in Psychology*, 1(1), 39-54.

SOLOVE, D. J. (2006): "A Taxonomy of Privacy", *University of Pennsylvania Law Review*, 154(3), 477.

TRUBOW, G. (1992): "Personal privacy and secondary-use dilemma (social aspects of automation)", *Software, IEEE*, 9(4), 73-74.

WESTIN, A. F. (1967): *Privacy and Freedom*, New York: Athenaeum.

WHITLEY, E. A. & KANELLOPOULOU, N. (2010): "Privacy and Informed Consent in Online Interactions: Evidence from Expert Focus Groups", Thirty First International Conference on Information Systems. St. Louis: AISeL.

http://aisel.aisnet.org/icis2010_submissions/126

WHO (2012): *World Health Statics 2012. France*, WHO Library Cataloguing-in-Publication Data.

WILTON, R. (2008): "Identity and privacy in the digital age", International Journal of Intellectual Property Management, 2(4), 411 428.

YIN, R. K. (2009): *Case Study Research: Design and Methods* (4th ed., Vol. 5), UK: Sage.

ZALLONE, R. (2010): "The Privacy Paradox or How I Learned to Have Rights that Never Quite Seem to Work", AAAI Spring Symposium Series, pp. 199-202, Palo Alto, California.

Paper 5

Building Trusted National Identity Management Systems:

Presenting the Privacy Concern-Trust (PCT) Model

Joseph Kwame Adjei & Henning Olesen

Center for Communication, Media and Information Technologies (CMI)
Aalborg University Copenhagen
A. C. Meyers Vænge 15, DK-2450 Copenhagen, Denmark
e-mail: {adjei,olesen}@cmi.aau.dk

Abstract—This paper discusses the effect of trust and information privacy concerns on citizens' attitude towards national identity management systems. We propose the privacy-concerns-trust model, which shows the role of trust in mediating and moderating citizens' attitude towards identity management systems. We adopted a qualitative research approach in our analysis of data that was gathered through a series of interviews and a stakeholder workshop in Ghana. Our findings indicate that, beyond the threshold level of trust, societal information privacy concern is low; hence, trust is high, thereby encouraging further institutional collaboration and acceptance of citizens' informational self-determination.

Keywords-Identity Management; PCT Curve; Privacy Concern; Trust; Trusted Identities.

Introduction

Although digital Identity Management (IdM) is fundamental to electronic government, globally, its implementation and adoption by citizens usually presents complex issues for its many stakeholders. The complexity has been attributed to the fact that it transcends technological issues as well as policy, legal, institutional, and economic aspects of society. The complexity is also compounded by the rate, at which standards and technological solutions become obsolete; the flexibility and ease of collection, use, dissemination of data; and the increased linkability of information to the data subject. This raises the potential for privacy concerns [1].

Ironically, previous privacy research has shown that individuals disclose personal information in exchange for some economic or social benefit subject to the "privacy calculus", an assessment that their personal information will subsequently be used fairly, and that they will not suffer negative consequences [2]. Moreover, where individuals can exercise some degree of control over data collection and use; information is collected in the context of an existing relationship; the information collected or used is relevant to the transaction; and they believe the information will be used to draw reliable and valid inferences about them; citizens are less

likely to raise concerns. Unfortunately, this is usually not the case. These phenomena often occur without direct involvement or control of the data subjects.

Governments in many countries have implemented some form of identity management as a critical enabler of government to citizens' interactions, and in the facilitation of business transactions. Unfortunately, the costs of implementations are usually not matched by the benefits and citizens' adoption of the expected or improvement in public services. This makes it difficult for governments to justify the implementation, since it often leads to embarrassment [3, 4].

In spite of its use being lower than expected, identity management can play a leading role, if the factors that affect its takeoff are properly addressed. Trusted identities ecosystems have been found to be very critical to the success of digital IdMS. This research focuses on understanding the key stakeholder concerns on information privacy in regards to the collection, storage, use, and transmission of personal identity information [5], and how such concerns should be addressed to ensure trusted identities.

The rest of the paper is organized as follows; the next section discusses the theoretical background for trust and privacy concerns, followed by a description of our research design and methods. We then discuss our findings from the stakeholder workshop and the interviews. We present our conclusions and recommendations for further studies in the final part of the paper.

Theoretical Background

The growing deployment of innovative systems for collecting, processing, and sharing personally-identifiable information place data subjects in a vulnerable situation and has a propensity to undermine confidence in identity management systems. A 2012 Europe-wide survey [6] revealed that online users are naturally concerned about risks in online transactions, and that users are not in control of their personal information disclosed on the Internet. The survey also revealed that users employ a variety of offline and online methods to protect their identity; 62 % of users better understand how to protect their identity in the offline transactions using data minimization techniques, whilst 90% trust national institutions and banks more than Internet service providers and e-shops [6]. Such observations cannot be true in many developing countries.

In developing countries many of the electronic government projects are viewed with suspicion with very low level of trust in the institutions that manage credentials. The source documents required for proofs of identities, i.e., civil registration systems are often unreliable [7] due to several instances of multiple registrations and enrollments of unqualified people. Busi-

nesses, usually, have difficulties in verifying the authenticity of credentials individuals presented for access to services. Credentials can in many instances only be verified manually, resulting in undue delays and customer frustration with its attendant privacy information implications.

Information Privacy Concerns

The issue of privacy is generally based on cognitive perceptions rather than on rational assessments. Privacy concern has been used as a key privacy construct by researchers [8, 9]. Smith et al. [10] developed the concern for information privacy (CFIP) model for operationalizing privacy concerns based on data collection, errors, secondary use, and unauthorized access to information or invasion. Collection, use and transmission of personal information by identity providers and relying parties must in principle be based on tacit or explicit consent by service providers to protect the interest of data subjects [2]. Citizens, therefore, become apprehensive, when their interests are not observed, or the perceived risk of the abuse exceeds the benefits derived from such implied social contracts.

These tensions between organizational use of personal information and societal information privacy concern are very topical in privacy research [11]. Previous studies have defined privacy as *the ability of an individual to exercise some degree of control of the access that others have to their personal information* [12]. Privacy is at risk, if individuals are unable to exercise control over their personal information during social interactions and business transactions (Solove, 2006; Clarke R. , 1999), and it is therefore disheartening for privacy-aware citizens to find out that inaccurate, out-dated, excessive or irrelevant data about them are stored by others.

Information privacy concerns can be categorised as

- *Illegitimate use of information [10], and*
- *Secondary use of personal information without the consent of the data subject, for purposes outside the primary reason for data collection [1].*

Therefore, it is imperative that organizations develop information practices that address the perceived risks and citizens concerns in order to project an innate trust (Mayer, Davis, & Schoorman, 1995; Adjei & Olesen, 2011). Although privacy concerns are almost always measured at an individual level of analysis, societal concern (overall privacy concerns of a nation) should reflect the concerns of its citizens and organizations [17, 18]. Various governmental interventions like regulations and controls are implemented to address societal information privacy concerns. Although Bélanger & Crossler [17] and others have discussed the

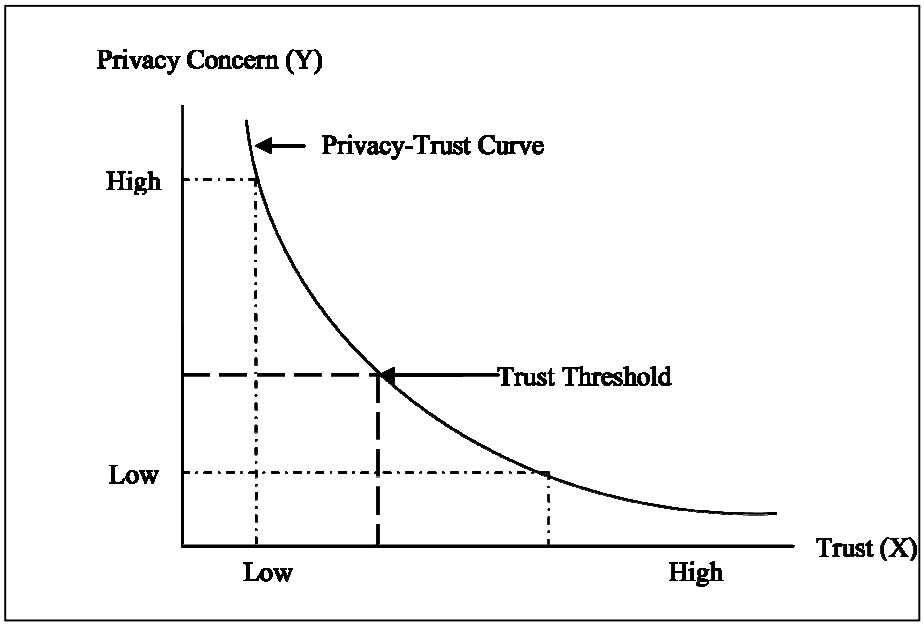


Figure 1: Qualitative relationship between privacy concern and trust.

privacy concern, there is still a need to clarify *how privacy concern and trust affect each other within the context of identity management.* This is one of the objectives of this study.

Trust

Trust plays an important role in societal discourses and attitudes towards electronic identification systems. Due process requires that organizations apply best practices in data acquisition and also strive to prevent illegitimate access by others to personal data in their custody. Bhattacharya et al. [19] describes trust as having a multidimensional construct and defined trust as an expectancy of positive or nonnegative outcomes that one can receive based on the expected action of another party in an interaction characterized by uncertainty [19]. Broadly, trust is considered as a firm belief in the reliability, competence, qualification, ability, strength, integrity, truthfulness, honesty, sincerity, and loyalty of the other party to transaction or interaction [20].

In their study on "an alternative model of trust", Mayer et al. [15] modelled the concept of trust by categorizing the key attributes of trustworthiness as the trustees' ability to fulfil the trusting action, the benevolence of trustees' intentions, and their integrity [15, 21]. Their definition was based on one person's beliefs about the characteristics of another person. In effect, trustworthiness can be operationalized using these three attributes of the trustee. Ability signifies competence or perceived expertise, business sense and judgement. Consistency, fairness and reliability describe integrity, whereas loyalty, openness and availability signify benevolence (Mayer, Davis, & Schoorman, 1995; Adjei & Olesen, 2011). These attributes are important determinants of the success of IdMS, since it can affect the usage behaviours of the systems.

A trust relationship is made up of three elements – the truster, the trustee, and the context in which trust is conferred [20]. Trusters are the citizens and relying parties, the trustees are the credential issuers and service providers, and the context is an IdMS or the electronic identity card scheme.

Perception of trust can be either due to the technology or the institutions [22]. A low citizens trust in credentials issuers and IdMS will be a major disincentive to accept the IdMS, since there is lack of identity assurance [23]. Such lack of trust can lead to unfavourable outcomes of the IdMS. Likewise, a low trust in credential issuers coupled with a high trust in the technology leads to a situation, where citizens might use technology as a competitive tool against the unpredictable and sporadic results. In such a scenario the IdMS will be viewed with suspicion and cynicism by the citizens [24, 22].

Relationship Between Trust and Privacy Concern

Various studies have established a relationship between trust and people's willingness to forgo their privacy concerns [25, 26]. What is not certain is the nature of the relationship between privacy, trust and societal attitude towards identity management systems. Trust is known to be a mediator between privacy concerns and behaviour [26, 27]. Thus, trust (the mediator) is what explains the effect that privacy concern (independent or predictor variable) has on societal attitude (the dependent or criterion variable). For instance, a correlation between income and cancer might be explained by a correlation between income and smoking (the mediator), and then between smoking and cancer. Thus, according to mediation models, privacy has little or no direct effect on behaviour; instead any effect can be explained by the links between privacy and trust, and then between trust and behaviour.

The relationship between privacy concern and trust can also be explained using the concept of moderation [28]. Moderators are variables that affect the directions and strengths of a relationship between an independent and a dependent variable [28]. Thus, in the case of privacy and trust, where there is high trust, privacy concern exerts an influence on behaviour, while in low trust environments privacy concern may have a negligible impact on behaviour, since behaviour is limited by the lack of trust. This study explains mediator and moderator relationships between privacy concerns, trust and citizens' attitudes towards national identity management systems.

Modelling Identity

Wilton [29] described digital identity as the relationship of idenenrollmenteen a person at the time of enrolment, and a person at the time of authentication [29]. Thus, identity is not just a

snapshot of a person, but part of a process from enrollment and credential issue of credential presentation, authentication and revocation [29]. When such a process is not followed or abused, citizens become concerned and lose confidence in the system or the identity service providers.

Privacy Concern-Trust Curve

Generally, societal interactions and business relationships begin from a low level of trust (distrust) and high privacy concern. With disclosure of more information, strong institutional cooperation and user awareness, users are able to exercise some degree of user control over their personal information, resulting in the establishment of a certain level of trust. Thus, citizens become more empowered and revise their negative perceptions about the IdMS and identity service providers. This establishment of trust reduces the initial privacy concerns. Thus, a high privacy concern is associated with low level of trust, and reduction in privacy concern results in an increase in trust. In other words, the mediating and moderating effect of trust can result in either a negative or positive societal attitude changes towards IdMS.

The qualitative relationship between trust and privacy concern is shown in Fig. 1. A certain threshold level of trust must be overcome, before the citizens are ready to open up for interaction. The figure also shows that absolute trust or zero privacy concern is not possible within a trusted identities environment, and hence the curve can only asymptotically approach the two axes. The purpose of the trust framework therefore is for society to establish the framework that can overcome the trust threshold. Beyond this level, trust and privacy is adequate to encourage more collaboration, creation of new identity-based services, institutional collaboration, etc.

Research Design and Methods

This study entailed two main phases – an exploratory phase, which saw the development of the model based on literature, and a qualitative based confirmatory phase, which was used to evaluate the model. The conceptual model on the basis of theoretical considerations is part of an on-going research project that seeks to present a reliable and valid instrument for measuring trusted identities ecosystem. The exploratory phase of the study was organized in line with two-step approach for operationalizing constructs and identifying measures [30]. Due to the multi-stakeholder nature of trusted national identities, we decided to adopt a research approach that engages the key actors and hence a qualitative methodological approach was deemed the most appropriate means for data collection from a societal perspective [31, 32]. We also applied the concepts of Interpretative Phenomenological Analysis [33] in our data

analysis because of its usefulness in understanding the experiences of individuals. The overarching research question was *"what are the key requirements for crafting a trusted identities ecosystem"*.

Stakeholder Workshop

Given the societal level of analysis, a stakeholder workshop was organized in Accra, Ghana.

All the major stakeholders involved in the collection, storage, use and issue of identity were represented, including Registrar of Births & Death, The Passport Office, Driver and Vehicle Licensing Agency (DVLA), National Identification Authority (NIA), National Health Insurance Authority (NHIA), Electoral Commission (EC), Ghana Revenue Authority, financial

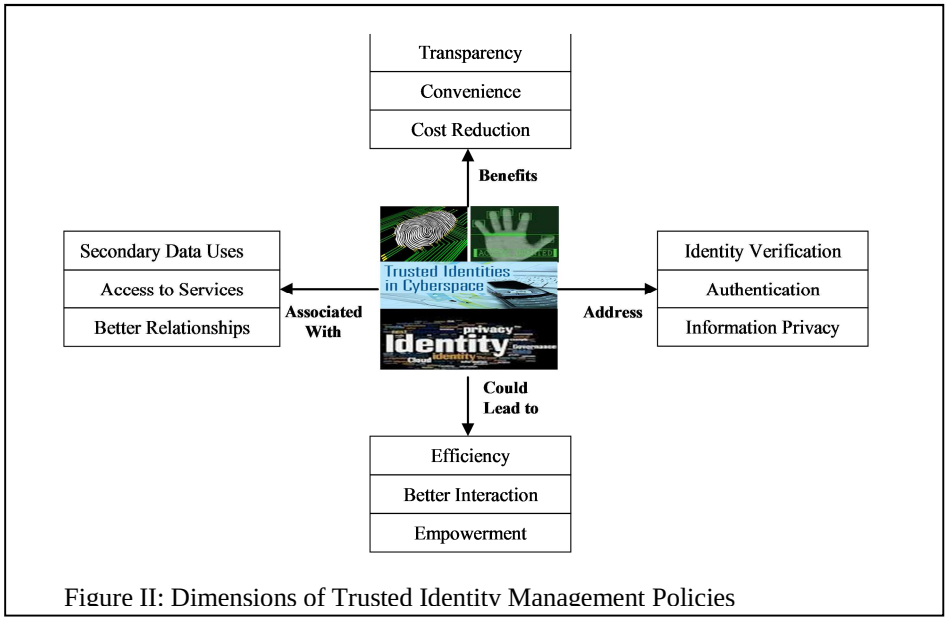


Figure II: Dimensions of Trusted Identity Management Policies

institutions and identity-related businesses, academic institutions, national institutions and non-governmental organisations involved in civil right advocacy, and the general public. The identification challenges in Ghana are considered to be typical of many developing countries.

During the workshop participants were offered the opportunity to discuss a number of prepared questions and scenarios. To inform discussions, participants listened to presentations on various aspects of trust, privacy and secondary uses of personal information. The presentations also highlighted the key concepts of trusted identities and the policy, technological and regulatory implications as well as related IdMS research and practices in OECD countries [34, 35]. The ideal situation as illustrated on Figure 2 was used to explain the benefits of trusted identities.

Some of the discussion questions were:

1. *What are the potential benefits and risks regarding the secondary uses of personal information?*
2. *What are the major challenges in relying on existing credentials presented for access to services?*
3. *How can institutional cooperation be encouraged given the conflicting regulations?*
4. *What attributes do citizens look for before trusting organizations with respect to secondary use of personal information?*
5. *What can be done to address issues arising from inappropriate use and/or exploitation of personal information?*
6. *What regulations, legislation, and/or policies are needed to address the evolving challenges?*

Interviews

A series of stakeholder interviews were conducted before and after the workshop. The pre-workshop interviews were made to identify the key issues and challenges from different perspectives. This helped in choosing and phrasing the discussion questions for the stakeholder workshop. The follow-up interviews were conducted to clarify some of the points raised during the workshop to solicit for further information. Interviewees included the officials of identity issuers, policy makers, journalists, private businesses involved in identity verification, and identity card manufacturers.

Transcription and Coding

Although raw data can sometimes be of interest in research they do not usually help the reader to understand the world under scrutiny and participants' views without a systematic analysis to illuminate the situation under investigation [36]. Transcripts were thus initially coded to aid meaningful analysis. Data coding, which is an important part of analysis, involves subdividing data into chunks of varying-sized words, phrases, sentences or whole paragraphs, and assigning categories [37]. Thus, codes are labels for allocating units of meaning to descriptive or inferential information compiled during a study. One of the key objectives of our coding approach is to identify relevant examples of the phenomena and analysis of the phenomena to discover distinct patterns, differences and commonalities [37].

Transcript of the workshop discussions and the interviews, in the form of audio-visual recordings, interview notes and summary of discussion sessions, were produced by the authors. The introductory background of speakers and interviewees were, however, included for coding and analysis purposes. This was meant to maintain speaker anonymity. No attempt was made to identify speech patterns, since that was not the focus of our research. The nature of the dis-

cussions and interviews was such that initial coding would not have been helpful since participant interviewees were from diverse backgrounds, and opinions were varied. Each of the transcripts was coded on the basis of the background of the various speakers, since each of the participants and interviewees were told to introduce themselves before speaking. This served as basis for coding and sub-categorization of the transcript.

Discussion of Findings

Societal Concerns

Comments and statements made by participants during the interviews and workshop revealed a number of societal concerns and the various sources of them. Some of the concerns are listed below:

- "*The identity agencies are only there to please their political party and not because they are skilled".*
- *"If the electoral commission knew what they are doing, why will they opt for a biometric system without a means of verification"?*
- *"The information on the National Identification Authority website is so scanty that I have no idea what is going on."*
- *"I wonder if the officials of the identification agencies read our emails or even if the emails get to the organisations in the first place, because they never respond to emails sent to addresses they have provided".*
- *"If I have a problem, I have no idea how to reach them by phone or on the Internet, except if I walk to their head office"*
- *"I do not know the use of all the information collected by many of the identification agencies. For instance, I do not understand, why my actual date of birth is stated on my driving license, when they could have simply stated that I am over eighteen or qualified to drive."*
- *"Since one can present different documents as proof of identity during voter registration or drivers' license acquisition, it gives room for multiple registrations."*

Such comments show the need for societal assurance that their opinions are taken seriously. In a situation, where citizens do not get responses for the concerns raised, it gives the impression that citizens are not involved in decisions that concern them. It is therefore important to empower citizens in order to generate commitment and contributions. In essence, when citizens' opinions are taken seriously, they feel that they are involved in decision-making and empowered, resulting in increased trust [38, 39].

Moreover, recruitment of unqualified personnel shows a lack of ability and integrity, which are all key attributes of trustworthiness [15, 40]. This is also manifested in comments like

- *"I always read stories in the dailies about impersonation and people making fake documents especially passports and birth certificates; many of the officials are involved".*

However, citizens would like to have informational self-determination - a sense of freedom to do what is interesting, personally important, and psychologically vitalizing [41]. Such concerns lead to distrust in government institutions and therefore very critical that the system for tracking vital source documents like birth and marriage certificates is improved. The key aspects of the civil registration that need to be made efficient include, birth, marriage and death registration.

Segregation of Personally Identifiable Information

Article 7.1 of the United Nations Convention on the Rights of the Child states that *"the child shall be registered immediately after birth and shall have the right from birth to a name, the right to acquire a nationality, and as far as possible, the right to know and be cared for by his or her parents"*. The birth certificate for instance contains the given name, surname (or family name), gender, date of birth, place of birth, and father and mother names. Given the importance of the birth certificate in the establishment of the core identity, its abuse in the form of multiple registration and registration of illegitimate people defeats its usefulness. If the birth registration system were to be strengthened, it could act as the basic document that all residents must rely on for initial registration.

The information on the birth certificate represents the 'Basic Identifier Set' (BIS) – information that can help identify a person and does not change over time [29]. Hence, the birth certificate can be a very useful document in addressing issues of multiple registrations, especially when individuals are made to use the number throughout life. In that case, enrolment of foreign nationals who reside in the country should be based on travel documents as part of the processing of residence permit.

Certain transactions requiring proofs of additional information might require credentials that show the individual's Personally Identifiable Information (PII) – additional information that is useful for identifying a person but may change over time, such as addresses, marital status, physical characteristics like height, hair/eye colour, or complexion [29]. The PII provides additional information that can typically not be found in the BIS. For border control purposes passport may be preferred more than a birth certificate. In other sector-specific transactions and interactions, other attribute data are necessary for effective identity verification. This kind of data is information that on its own might not be able to identify a person, but will provide important traces when linked to either the BIS or PII data, or when such data are aggregated over time and space (e.g. healthcare records, tax return information, driver's and vehicle li-

cence, banking and insurance information. Given the sometimes sensitive nature of such information, e.g. health records, it might require additional level of security to avoid linkability to the BIS and PII. In essence, other attribute data are identity-related, albeit 'sector-specific',

Strong Focus on Identity and not Credentials

A common misunderstanding on the part of credential issuers and policy makers during the workshop was the equation of strong credentials to efficient identity management systems. This became apparent from statements like *"we have introduced biometric based ID cards that are difficult to forge"*.

There is, therefore, the need to move away from credentials towards unique identification. A credential such as a passport or driving licence typically includes some items from each of the three aspects of identity – the BIS, PII such as height, eye colour, and some sector-specific data such as entitlement to drive specific classes of vehicle, or visas indicating entitlement to enter a specific country. This is illustrated on Fig. 3.

A distinct feature of a credential is that it encapsulates attributes and entitlements in a reliably verifiable form. There is therefore the tendency to equate such documents as representing the identity of a person when in fact they might not be representative in a given context. For instance, passports and driving licences have historically been presented as foolproof documents loaded with the necessary information that can enable the holder to access services and for authentication purposes. This is not without drawbacks, since it is susceptible to revealing more information about the holder than is necessary in any given authentication context. Using a passport for proof of age will no doubt reveal the passport holder's name, place of birth and citizenship, and a driver's licence used for similar purpose can also reveal your date of birth and address.

A focus on identity will also make it easier to enforce policies appropriate to the data in question, particularly when different sector-specific data items entail different policy controls. For instance, entitlement to drive a vehicle may not be part of major privacy concern, whereas credit status will, hence data security policies could be segregated to address such data. On the other hand, since healthcare history and medical conditions are very sensitive, a different set of policies will apply. Graphically, one might think of this as the ability to segregate identity data into sector-specific segments and cater for discrete management policies by sector and data type (cf. Fig. 3). Thus, within a given data segment, assertions of identity ('the holder of this credential is XX') may make one kind of data security policy appropriate, while

assertions of other attributes ('the holder of this credential has been treated for Repetitive Stress Injury') may require quite different policy treatment.

Application of Privacy Enhancing Tools

Various privacy-enhancing and minimal disclosure technologies have been tested that address the requirement not to reveal unnecessary details in transactions.

For instance, the touch2ID biometric application allows users to prove their age without storing or revealing extra details about the individual [42]. Similarly, the ABC4Trust project has released and tested guidelines for implementing attribute-based credential technologies focusing on trust, based on Idemix and U-prove technologies [43, 44, 45].

In an online context disclosure of excess data can be avoided. Credentials can realistically encapsulate just those data items, which serve to uniquely identify the holder (such as the BIS), as long as they provide a way of linking to the rest of the holder's personal data, which may be held elsewhere. In other words, the option now exists to make use of the distributed nature of networked computing, so as to allow much more flexible 'placement' of identity data of different types. This is valuable in terms of policy control, because it makes it possible

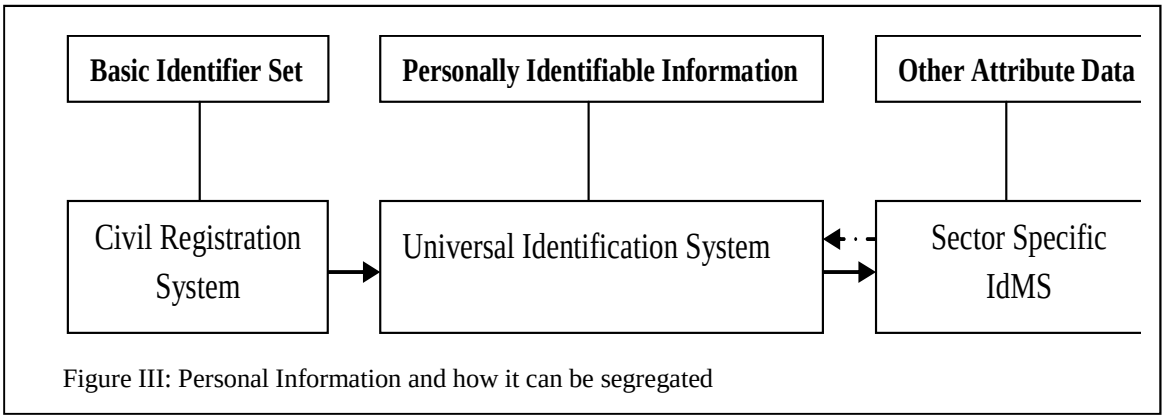


Figure III: Personal Information and how it can be segregated

to apply controls at the place where the data is held, rather than trying to enforce it wherever the credentials are verified.

Encouraging Trusted Environment

Trust is what moderates and mediates citizens' privacy concerns and attitudes towards IdMS. Thus, individuals are likely to engage in transactions, if their level of trust exceeds their personal privacy concern threshold, which is reached, when the potential benefits outweigh the risks. This threshold will always depend on the type of transaction and the amount of identifiable information revealed. For instance, transactions requiring the revelation of other attribute data might require a lower trust threshold. Thus, when positive steps (i.e., data minimisation)

are taken to improve the IdMS, the moderation effect of trust will cause citizens to revise their attitude towards the IdMS, leading to more trust in the credential issuers and the technology and thereby moving down and to the right on the trust threshold. Similarly any negative actions on the part of credential issuers will increase the privacy concern and thereby causing a move upwards and to the left on the privacy trust curve. The trusted identities framework in the United States, where the interest of all stakeholders in the identity ecosystems are taken into account, is a clear step taken by the US government to increase trust [35].

Conclusions and Future Research

This paper discussed the issues and challenges associated with accountable management of personal identifiable information and the provision of more user control over personal information. The findings from this study suggest that information privacy concerns can affect the posture of society in relation to attitudes and preferences for regulatory environments and willingness to accept a particular identity management system [8, 18, 46, 26]. We also highlighted the relationship between information privacy concern and trust from a societal perspective, and its effect on trusted identity management systems.

Our findings show that the unreliable civil registration system can be a major reason for such concerns. Given that the civil register is in many instances a key source document for credential acquisition, its unreliability leads to all kinds of credential abuses. Hence, governments especially in developing countries must focus on strengthening the civil registration system in order to avert such abuses of personal identity information.

Our work clearly shows the two steps towards establishment of a trusted national framework, which are typical for the situation in many developing countries. Initially, trust is low and privacy concerns are high, because of poor implementations, but once the initial problems are identified and addressed, it is possible to meet a threshold level of trust, thereby reducing privacy concerns and paving the way for effective business transactions and societal interaction. This is the point at which societal trust in Identity service providers is high enough to encourage institutional collaboration [22], and citizens' informational self-determination [41]. We also highlight the need for policy makers to categorise personal information in a way that will encourage secondary uses of personal information whilst ensuring that sensitive personal information is released only to legitimate people.

This study focused mainly on citizens' attitudes towards identification systems in Ghana and that poses a number of issues in terms of generalizability that will need to be tested. For instance, there are peculiar dynamics pertaining to every country and for that matter the infer-

ences drawn might not be representative for all developing countries. Moreover, the use of a qualitative research approach also gives room for inferences that are not tested empirically, as is the case of quantitative research. In the future it will be interesting to examine quantitatively the relationship between trust and privacy concerns in relation to citizens' attitudes towards identity management systems.

REFERENCES

[1] M. J. Culnan, "How Did They Get My Name?: An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use," MIS Quarterly, vol. 17, no. 3, pp. 341-363, 1993.

[2] P. H. Jos, "Social Contract Theory: Implications for Professional Ethics," The American Review of Public Administration, vol. 36, pp. 139-155, June 2006.

[3] E. A. Whitley and G. Hosein, "Global Identity Policies and Technology: Do we Understand the Question?," Global Policy, vol. 1, no. 2, May 2010.

[4] P. Seltsikas and R. M. O'Keefe, "Expectations and outcomes in electronic identity management: the role of trust and public value," European Journal of Information Systems, vol. 19, pp. 93–103, 2010.

[5] C. J. Bennett and C. D. Raab, The Governance of Privacy Policy Instruments in Global Perspective, Aldershot: Ashgate, 2003.

[6] W. Lusoli, M. Bacigalupo, F. Lupiañez, N. Andrade, S. Monteleone and I. Maghiros, "Pan-European Survey of Practices, Attitudes and Policy Preferences as regards Personal Identity Data Management," European Commission JRC Scientific and Policy Reports, Luxembourg, 2012.

[7] WHO, "World Health Statics 2012," WHO Library Cataloguing-in-Publication Data, France, 2012.

[8] J. H. Smith and T. Dinev, "Information Privacy Research: An Interdisciplinary Review," MIS Quarterly, vol. 35, no. 4, December 2011.

[9] K. A. Stewart and A. H. Segars, "An Empirical Examination of the Concern for Information Privacy Instrument," Information Systems Research, vol. 13, no. 1, pp. 36-49, March 2002.

[10] H. J. Smith, S. Milberg and S. Burke, "Information privacy: Measuring individuals' concerns about organizational practices," MIS Quarterly, vol. 20, no. 2, pp. 167–196, 1996.

[11] R. Mason, "Four Ethical Issues of the Information Age," MIS Quarterly, vol. 10, no. 1, pp. 4-12, 1986.

[12] A. F. Westin, Privacy and Freedom, New York: Athenaeum, 1967.

[13] D. J. Solove, "A Taxonomy of Privacy," University of Pennsylvania Law Review, vol. 154, no. 3, pp. 477, 2006.

[14] R. Clarke, "Internet privacy concerns confirm the case for intervention," Communications of the ACM, vol. 42, no. 2, pp. 60-67, February 1999.

[15] R. C. Mayer, J. H. Davis and D. F. Schoorman, "An Integrative Model of Organizational Trust," The Academy of Management Review, vol. 20, no. 3, pp. 709-734, July 1995.

[16] J. K. Adjei and H. Olesen, “Keeping Identity Private,” Vehicular Technology Magazine, IEEE, vol. 6, no. 3, pp. 70-79, September 2011.

[17] F. Bélanger and R. E. Crossler, “MIS Quarterly,” Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems, vol. 35, no. 4, pp. 1017-1041, December 2011.

[18] P. A. Pavlou, “State of the Information Privacy Literature: Where are we now and whee should we go?,” MIS Quarterly, vol. 35, no. 4, pp. 977-988, 2011.

[19] R. Bhattacharya, T. M. Devinney and M. Madan, “A formal model of trust based on outcomes,” The Academy of Management Review, vol. 23, no. 3, pp. 459-472, July 1998.

[20] WP17, “D17.4: Trust and Identification in the Light of Virtual Persons,” FIDIS, 2009.

[21] A. N. Joinson, “Privacy Concerns, Trust in Government and Attitudes to Identity Cards in the United Kingdom,” Proceedings of the 42nd Hawaii International Conference on System Sciences, 2009.

[22] T. S. Teo, S. C. Srivastava and L. Jian, “Trust and Electronic Government Success: An Empirical Study,” Journal of Management Information Systems, vol. 25, no. 3, pp. 99–131, 2008.

[23] S. J. Crosby, “Challenges and Opportunities in Identity Assurance,” March 2008. [Online].Available: http://www.hm-treasury.gov.uk/media/6/7/identity_assurance060308.pdf.

[24] S. Srivastava and T. Teo, “Citizen trust development for e government adoption: Case of Singapore,” in Ninth Pacific Asia Conference on Information Systems, Bangkok,, 2005.

[25] M. J. Culnan and P. K. Armstrong, “Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation,” Organization Science, vol. 10, no. 1, pp. 104-115, 1999.

[26] N. K. Malhotra, S. S. Kim and J. Agarwal, “Internet Users’ Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model,” Information Systems Research, vol. 15, no. 4, pp. 336-355, 2004.

[27] J. Nickel and H. Schaumburg, “Electronic privacy, trust and self-disclosure in e-recruitment. In extended abstracts on Human factors in computing systems,” in , New York, USA, 2004.

[28] R. M. Baron and D. A. Kenny, “The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations,” Journal of Personality and Social Psychology, vol. 51, no. 6, pp. 1173-1182, 1986.

[29] R. Wilton, “Identity and privacy in the digital age,” International Journal of Intellectual Property Management, vol. 2, no. 4, pp. 411 428, 01-01 2008.

[30] A. Burton-Jones and D. W. J. Straub, “Reconceptualizing System Usage: An Approach and Empirical Test,” Information Systems Research, vol. 17, no. 3, pp. 228–246, September 2006.

[31] J. W. Creswell, Qualitative inquiry and research design: Choosing among five approaches, 2nd ed., Thousand Oaks, CA: Sage Publications, 2007.

[32] R. K. Yin, Qualitative Research from Start to Finish, New York: The Guildford Press, 2011.

[33] J. A. Smith, “Reflecting on the development of interpretative phenomenological analysis and its contribution to qualitative research in psychology,” Qualitative Research in Psychology, vol. 1, no. 1, pp. 39-54, 2004.

[34] OECD, 2011. [Online]. Available: http://dx.doi.org/10.1787/5kg1zqsm3pns-en.

[35] NSTIC, "National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy April 2011," The White House , Washington, 2011.

[36] T. Basit, "Manual or electronic? The role of coding in qualitative data analysis," Educational Research, vol. 45, no. 2, pp. 143-154, 2003.

[37] I. Dey, Qualitative Data Analysis A User Friendly Guide for Social Scientists, London: Routledge, 2005.

[38] A. Wilkinson, "Empowerment: theory and practice," Personnel Review, vol. 27, no. 1, pp. 40-56, 1998.

[39] WHO, "WHO User empowerment in mental health – a statement by the WHO Regional Office for Europe," WHO Regional Europe, Copenhagen, 2010.

[40] R. Hardin, "The Street-Level Epistemology of Trust," Politics & Society, vol. 21, no. 4, pp. 505-529, 1993.

[41] E. Deci, J. Connell and R. Ryan, "Self-determination in a work organization," Journal of Applied Psychology, vol. 74, no. 4, pp. 580-590, 1989.

[42] C. Evry, "Proof-of-age scheme prepares to expand across Wiltshire," 2010. [Online]. Available: http://www.wiltshiretimes.co.uk/news/inyourtown/wiltshire/8239556.Proof_of_age_scheme_prepares_to_expand_across_Wiltshire/.

[43] J. Camenisch, I. Krontiris, A. Lehmann, G. Neven, C. Paquin, K. Rannenberg and H. Zwingelberg, "Architecture for Attribute-based Credential Technologies – Version 1," 2011.

[44] IBM_Research, "IDEMIX (Identity mixing) Project Overview," 2010. [Online]. Available: http://www.zurich.ibm.com/pri/projects/idemix.html. [Accessed 28th February 2012].

[45] Microsoft_Connect, "Microsoft U-Prove Community Technology Preview R2," 2010. [Online]. Available: https://connect.microsoft.com/site1188.

[46] F. D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," MIS Quarterly, vol. 13, no. 3, pp. 319-340., 1989.

Paper 6

Towards a Trusted National Identities Framework

Adjei, J. K. (2013). Towards a trusted national identities framework.

Info, Emerald, 15 (1), 48–60.

1 INTRODUCTION

Identity assurance and management play a critical role in modern business transactions, societal interactions as well as national security and border control. Its criticality is compounded by the interdependence of communication networks and its convergence with information technologies in cyberspace. This presents challenges, particularly to policy makers, law enforcement agencies and business executives in addressing the growing trend of identity fraud, other forms of identity abuses and misuse of personal information. The issue of trust is thus brought to the fore owing to its importance in communication (Giffin, 1967), institutional collaboration (Farrell and Knight, 2003), implementation of self-managed systems (Lawler, 1992) and in user empowerment (Smith, 2004). Trust is thus a key foundation of an effective identity ecosystem and is shaped by the confidence placed in the systems that create and manage user identities (NSTIC, 2011; Grant, 2011).

Trust is also an important step in the provision of identity assurance (EnCoRe, 2012; Crosby, 2008) to citizens and in instilling discipline in the use of personal information. In a trusted identities ecosystem all stakeholders can effectively collaborate with the assurance of a certain degree of trust and informational self-determination in their interactions and business transactions (NSTIC, 2011; Grant, 2011). The overarching question then is *"what are the key requirements for crafting a trusted identities ecosystem?"*

This paper addresses this research question using a trusted identities framework by adapting concepts from the DeLone and McLean information systems (IS) success model (DeLone & McLean, 2003). The IS success model has been applied to evaluate the contributing factors to information systems success at the individual and at organisational levels of analysis (Urbach and Müller, 2012; Petter, et al., 2008). However, trusted identities ecosystem is a multi-stakeholder issue and hence has societal level of analysis. We therefore introduce institutional co-operation and user empowerment to the DeLone and McLean IS success model as additional independent variables.

The paper is organised as follows. The paper begins with a brief background to the study and a discussion of the key concepts of trust, personal information uses and information privacy. A conceptual model of trusted identities framework is subsequently introduced followed by

the research design and methods. The results and discussion of the findings, which includes the privacy concern–trust curve and its implication on the trusted identities framework, is then presented. The last section presents our conclusions and opportunities for further research.

2 BACKGROUND

A Trusted Identities Ecosystem is a digital identity environment where individuals, organizations and services can trust each other because all participants in the ecosystem follow established standards for digital identity verification and authentication (NSTIC, 2011; Grant, 2011). The aim of an identity ecosystem is to provide better and more reliable assurances for digital identities both physically and online. In a trusted identity ecosystem, users have a high degree of assurance that their identity (business, social, health records) will be secure with a certain degree of physical and digital anonymity (NSTIC, 2011). "To craft such an environment, entities relying on claims information must be able to determine what assertions they require, the validity of the assertions and whether it is certified or supported with information about the credential or claim issuer."

The US government is spearheading a scheme to address which claims issuers would be designated as trustworthy as part of its "National Strategy for Trusted Identities in Cyberspace; Enhancing Online Choice, Efficiency, Security, and Privacy" (NSTIC, 2011) through an accreditation process. A key part of their strategy is the recommendations for a series of trust frameworks through interoperable policies. The strategy does not describe how a trust framework could be crafted to make the identity ecosystem successful. The strategy although laudable also focuses mainly on internet-based transactions as evidenced in its definition of an identity ecosystem (NSTIC, 2011). The strategy which is an attempt at democratisation of personal information use (Bradwell, 2010) seems laudable and governments in other countries might want to emulate it. However, many developing countries were still not able to deal with fundamental identification challenges. Primary uses of tokens and credentials are for physical verification, by the credential users in pursuit of their core objectives, with little room for identity assurance and real-time verification by third parties.

The identification challenges could in part be traced to the unreliable civil registration systems which are a key source for identity documents. For instance, in Ghana, birth registration coverage is only 71% according to WHO's 2012 Health Statistics Report (WHO, 2012) which indicates that close to a third of the nation's population are not registered. This challenges the reliability of identity tokens for secondary uses by businesses and government agencies. Existing identity management systems also remain heterogeneous and independently managed

identity silos with little involvement of users and service providers (Adjei and Olesen, 2011). Changes of address, update of personal details (e.g. surname change owing to marriage), cannot be handled seamlessly without going through each individual identity provider. Elections and landed property acquisitions are usually characterised by controversy because of the lack of trust in the identity authentication and verification. Such instances have resulted in a relatively low and declining level of citizens' trust in credential issuers and service providers (Hardin, 1993).

TABLE I
KEY CONCEPTS AND STAKEHOLDERS IN IDENTITY ECOSYSTEM

Concepts/Stakeholders	Description of Activities
Data Subjects (e.g. citizens)	Trustees in the trust framework. To be issued digital identities and credentials to complete transactions.
Identity Providers	Responsible for the processes involved in enrolling subjects in the system and issue of credentials. Referred to as trustors in the trust model.
Attribute Providers	Oversee the processes involved in creating, validating, and keeping up the attributes associated with identities. Could be either trustors or trustees in the trust model.
Relying Parties	Make transaction decisions based on the receipt of credentials. Trustees in the trust model.
Credential	Credential is a generic term that can apply to both paper documents like Passports or Birth Certificates, and non-paper based objects such as smartcards and other tokens.
Claims	A claim is a statement that a person, organization, etc (data subject) makes about itself or another subject e.g. name, date of birth citizenship, etc.

3 LITERATURE REVIEW

3.1 Trust

The concept of trust has been studied from different perspectives such as sociology, psychology, economics and political sciences but a willingness to take risks may be one of the

few characteristics common to all trust situations (Johnson-George and Swap, 1982; Mayer, et al., 1995). In the context of using personal identity information, parties are likely to act and react willingly. This is in line with the definition of trust as *"the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party"* (Mayer, et al., 1995). This presupposes that in the identity management process, data subjects are perceived to be in a vulnerable position and trust is what will induce parties to engage in transactions irrespective of the vulnerability levels. Thus, trust is the

probability that a party to a transaction will act in a way that is beneficial or at least not detrimental to the interest of the other party for the latter to cooperate (Gambetta, 1988). The above definitions make the differences between predictability and trust unclear and hence the need to situate trust in its proper context. Although the two are a means of reducing uncertainty, trust goes beyond predictability and hence reduction of uncertainties. Otherwise those who can consistently ignore the desires and intentions of trustors and act in their own self-interest can be deemed to be trusted, because of their predictability (Mayer, et al., 1995).

3.2 Trustworthiness

Trustworthiness can be better explained by reference to the three main actors in a trusting relationship – trustor, trustee and context (Kramer, 1999; FIDIS, 2009). In this study, *trustors* are the citizens (or virtual citizens since trust can also be a matter between virtual persons (Cofta, 2008)). The *trustees* are the credential issuers and relying parties and the *context* is the identification scheme. Trustworthiness is based on the attributes exhibited by the trustees within the context. Mayer et al, (1995) identified three important characteristics that help in building the foundation for the development of a trust framework (Mayer, et al., 1995). Ability, integrity and benevolence have been identified as the key characteristics of trustees in the trust development process. Ability signifies competences, perceived expertise, business acumen and judgement that enable the trustee to have influence within a particular domain. Benevolence on the other hand connotes the extent to which the trustee can be assured of going beyond the profit motive to serve the interest of the trustor. Essentially, benevolence suggests that the trustee will behave in a desirable manner towards a set objective, irrespective of their personal preferences (Rosen and Jerdee, 1977). Integrity is premised on the trustor having a positive perception that the trustee will adhere to a set of acceptable principles. Thus adherence to a set of moral principles accepted by the trustor defines personal integrity. The concept of trust and trustworthiness thus has multidimensional constructs of ability, integrity and benevolence. Ability is characterised by competence or perceived expertise; integrity signifying consistency, fairness and reliability; whereas loyalty, openness and availability describe benevolence (Mayer, et al., 1995; Adjei and Olesen, 2011). Therefore a trust relationship can be negatively affected when the trustee consistently provides wrong information, refuses to provide or delays in the delivery of personal information to a legitimate recipient, or provides legitimate information to the wrong persons. Hence, users' perception of trust towards an identity management system (IdMS) is an important determinant of its success as they can affect the usage behaviors of the systems.

3.3 Personal Information Uses and Privacy

Personal information comprises information that specifically identifies an individual (e.g. name, date of birth, address, telephone number, email address, or account number, their location, or activities on the Internet that can be linked to that person (Wilton, 2008). Thus it is any information describing a natural person or an identifiable individual (Trubow, 1992). Personal information uses have become central to the business models of the digital age, such as the management of government institutions; and to people's everyday lives and relationships (Bradwell, 2010). Such practices could offer user convenience, efficiency and personalisation but inherently requires collection of pieces of data subjects' personal attributes. Although such practices can be regarded as an "implied social contract" (Jos P. H., 2006) between service providers and users, there are a number of complex legal, privacy and trust issues regarding collection, storage and use of information for purposes other than the primary intention (Milne and Gordon, 1993). To feel private, data subjects must be able to trust credential issuers and service providers to prevent access by others, and to follow best practices and applicable laws in legitimate data acquisition. It is therefore a discomfort for a privacy-aware individual to find out that inaccurate, outdated, excessive and irrelevant data about them are stored by others (Raab, 2005).

Privacy in effect is the claim to or the right of individuals to exercise a measure of control over the collection, use and disclosure of their personal information (Adjei & Olesen, 2011; Pavlou P. A., 2011). However the Internet and allied information technologies continue to make the idea of assuming physical control over the collection and use very elusive given that data can easily be mishandled (Adjei and Olesen, 2011). Moreover, the concept of privacy has both collective and individual dimensions (Regan, 2002) given the privacy implications in accessing, storage, use and data sharing of data – information privacy. Clarke defined information privacy specifically as "the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves" (Clarke R. , 1994). Hence, information privacy refers to the claims of individuals that their personal data should generally not be available to others, and that, where data are possessed by another party, the individual must be able to exercise a substantial degree of control over the data and their use (Bélanger and Crossler, 2011).

Information privacy concerns in effect refer to the factors affecting a person's willingness to render personal information (Dinev and Paul, 2006), engage in online transaction activity (Pavlou, et al., 2007), and to comply with government regulations – such as enrolling in national IdMS programs or acceptance to be profiled (Milberg, Smith, & Burke, 2000; Pavlou P.

A., 2011). Generally, individuals are less likely to perceive information practices as privacy-invasive when (Culnan M. J., 1993; Clarke R. , 1994; Tolchinsky, et al., 1981):

- information is collected in the context of an existing relationship;
- they perceive that they have the ability to control future use of the information;
- the information collected or used is relevant to the transaction; and
- they believe the information will be used to draw reliable and valid inferences about them.

Hence users are likely to avoid using an IdMS if there is a perception that their personal information will be subjected to various forms of privacy abuses. It is therefore imperative that users are given privacy assurances in IdMS implementations. Such assurances could lead to enforcement of privacy regulations, user education and secure and trusted systems. The more individuals value privacy, the less control they perceive to have over their personal information and this will have a negative implication on trust (Stone, et al., 1983).

4 TRUSTED IDENTITIES FRAMEWORK

"When the agencies have vague or inconsistent goals (as is usually the case), what the workers do will be shaped by the circumstances they encounter at the job, the beliefs and experiences they bring to the job, or the external pressures on the job" (Wilson, 1989)

Many user-centric, privacy enhancing identity management systems models have been proposed (Microsoft_Connect, 2010; IBM_Research, 2010; NSTIC, 2011). A key aspect of these proposals is the need for user trust and trust frameworks to ensure the cooperation of all stakeholders within the identity ecosystem. We propose a conceptual model for a trusted identities framework based on the Delone and Mclean IS success model (see Figure I) since it has been used extensively to evaluate information systems success (DeLone & McLean, 1992; DeLone & McLean, The DeLone and McLean model of information systems success: a ten-year update, 2003). Many of its applications are within organisational or individual levels of analysis. Since national identities go beyond individual organisations within the ecosystem to become a societal issue, we adapted the model by examining the definition of the dimensions and excluded those that are not applicable to a trusted identities framework within a societal context. The following constructs are proposed:

- System quality must not only consider performance characteristics, functionality, and ease of use of the system but also the skill set of the people, availability of documentation and the reliability of the processes. This is in line with the definition of information systems, which is the combination of technology, people, procedures and pro-

cesses (O'Brien and Marakas, 2010). For instance, if the system has all the attributes as described in (DeLone & McLean, 2003) with no skilled personnel to run it or ineffective processes, the performance of the system can be affected as well as the trustee's relationship with the trustor.

- Information is said to be of good quality when it is useful, timely, cost effective, reliable and understandable. These are critical factors in identity management systems, and play a prominent role in affecting how all the stakeholders in the identities ecosystem trust the system and each other (Schaupp, et al., 2006; Petter, et al., 2008).
- User empowerment: this includes the extent of user participation in decision making, the user's ability to exercise a degree of control over their personal information or informational self-determination, and to have confidence that third parties respect their privacy (Biskup and Brüggemann, 1988). Previous research found that individuals who believe they can exert more control over events, such as the secondary use of personal information, are less likely to perceive that their privacy is being invaded (Tolchinsky, et al., 1981). When users are involved and empowered they are more likely to have positive attitudes toward secondary information use and hence will also have a lower concern for privacy. Deci et al (1989) have posited that self-determined individuals experience a sense of freedom to do what is interesting, personally important, and vitalizing (Deci, et al., 1989). User empowerment therefore leads to state of belief in individuals that they can influence the system of which they are an integral part.
- Institutional cooperation: This describes the aspects of key stakeholders working together to ensure interoperable laws, technologies, systems and standards. This type of collaboration also leads to effective communication and compliance with standards with the identities ecosystem.
- Service quality is used to measure the overall support that users receive from service providers. Key aspects of service quality; responsiveness, reliability, empathy, competence (DeLone & McLean, 2003; Urbach & Müller, 2012).
- Use, user satisfaction and net benefits: The trusted identities framework describes how stakeholders in the identity ecosystem (societal level of analysis) trust each other and not necessarily the use of the credentials or services by the service providers systems. Hence the use, user satisfaction and net benefit dimensions are not necessary in that respect since they are usually organisational associated (DeLone & McLean, 2003; Petter, DeLone, & McLean, 2008; Urbach & Müller, 2012). Instead we consider perceived trust and perceived privacy which then lead to trusted identities.

Where there is a positive perception of trust and privacy among the stakeholders in an identity ecosystem, and the services they provide, it can engender collaborative environment and more innovative use of personal information for secondary purposes.

FIGURE I
DELONE AND MCLEAN IS SUCCESS MODEL (DELONE AND MCLEAN, 2003)

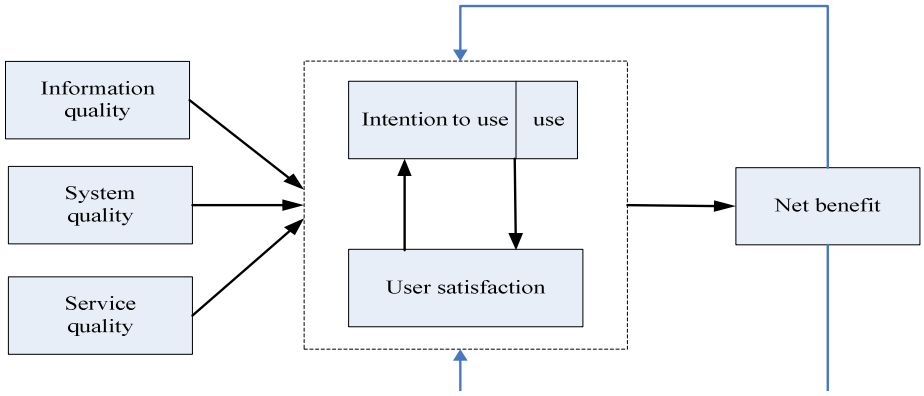
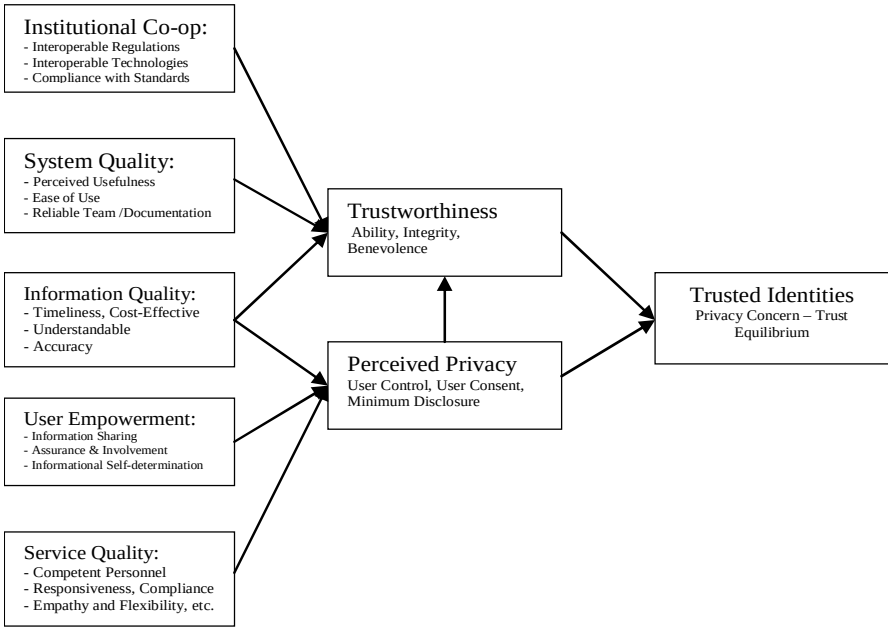


Figure II describes the trusted identities framework. Institutional cooperation has a positive influence on trustworthiness. Interoperable laws, technologies, policies and standard are typical examples of institutional cooperation. Also, strict enforcement of regulation and ability to seek redress are also signs of institutional cooperation. Systems quality and information quality have also a positive relationship with trustworthiness. Usefulness and ease of use (Davis, 1989; DeLone & McLean, 2003) skilled and reliable credential issuers signify their abilities whilst information signifies integrity on the part of the identity and relying parties. These are the attributes of trustworthiness (Mayer, et al., 1995; Adjei and Olesen, 2011). User empowerment, information quality and service quality have the potential of minimizing societal privacy concerns. Positive societal privacy concerns are signs that identity and service providers are benevolent – which is an attribute of trustworthiness. Trustworthiness and positive privacy concerns result in a trusted identities ecosystem.

FIGURE II
TRUSTED IDENTITIES FRAMEWORK



5 RESEARCH DESIGN AND METHODS

This study comprises two main phases – an exploratory phase, which saw the development of the model based on literature and a qualitative based confirmatory phase which was used to evaluate the model. The conceptual model on the basis of the theoretical consideration is part of an ongoing research project that seeks to present a reliable and valid instrument for measuring trusted identities ecosystems. The exploratory phase of the study was organised in line with the two-step approach (Burton-Jones and Straub, 2006) for operationalising constructs and identifying measures. Owing to the multi-stakeholder nature of trusted national identities, we decided to adopt a research approach that engages the key actors and hence a qualitative methodological approach was deemed the most appropriate means for data collection (Creswell, 2007; Yin, 2011) by means of stakeholder interviews and a workshop/forum. We also applied the concepts of Interpretative Phenomenological Analysis (Smith, 2004) in our data analysis because of its usefulness in understanding the experiences of individuals. The overarching research question was *"what are the key requirements for crafting a trusted identities ecosystem"*.

Stakeholder Workshop

The stakeholder workshop was organised in Accra, Ghana, during which participants were offered the opportunity to discuss a number of prepared questions and to listen to presentations on issues ranging from secondary issues of personal information and trusted national identities. The workshop convened on January 16, 2012, in an auditorium at Ghana Telecom

University College (GTUC), Accra. Accra was chosen mainly because the identification challenges in Ghana typifies many developing countries with respect to secondary uses of personal information, privacy concern and trust. The workshop brought together all the major national institutions involved in the collection and storage of personal information, such as the Registrar of Births and Death, The Passport Office, Driver and Vehicle Licensing Agency (DVLA), National Identification Authority (NIA), National Health Insurance Authority (NHIA), Electoral Commission (EC), Ghana Revenue Authority, financial institutions, biometric and identity-related businesses, academic institutions, national institutions and non-governmental organisations involved in civil right advocacy, and the general public. To inform discussions participants were given background information and copies of the discussion questions during a presentation on privacy and identity management. The presentation highlighted the key concepts on identity management, including major policy, technological and regulatory issues and related IdMS research and practices in OECD countries (OECD, 2009; NSTIC, 2011; OECD, 2011). Participants were given copies of the prepared questions and key issues raised. The facilitator asked questions and invited participants to speak about the issues and share their experiences and any reservations they might have. Where particular issues or questions were sector-specific, the agencies concerned were given the opportunity to respond to such questions. Discussion questions included:

1. What are the potential benefits and risks regarding the secondary uses of personal information?
2. What are the major challenges in relying on existing claims and credentials presented for access to services?
3. How can institutional cooperation be encouraged given the conflicting regulations?
4. What are the evolving public trust issues with respect to secondary use of personal information?
5. What problems may develop as innovative technologies enhance the ability and ease of widespread personal data sharing for secondary purpose and commercial uses?
6. What can be done to address issues arising from inappropriate use and/or exploitation of personal information?
7. What regulations, legislation, and/or policies are needed to address the evolving challenges?

Interviews

A series of stakeholder interviews were conducted before and after the workshop. The pre-workshop interviews were used in identifying the key issues and challenges from different stakeholder perspectives. It helped in choosing and phrasing the discussion questions for the

stakeholder workshop. Follow-up interviews were conducted to clarify some of the points raised during the workshop and to solicit further information. Interviewees included officials of identity issuers, policy makers, journalists, private businesses involved in identity verification, and identity card manufacturers.

Transcription and Coding

A transcript of the workshop discussions and the interviews, in the form of audio-visual recordings, interview notes and a summary of discussion sessions were produced. The introductory background of the speakers and interviewees were included for coding and analysis purposes. This was meant to maintain speaker anonymity. No attempt was also made to identify speech patterns, since that was not the focus of our research. The nature of the discussions and interviews were such that initial coding would not have been helpful since participant interviewees were from diverse background and opinions were varied. Each of the transcripts was coded on the basis of the background of the various speakers since each of the participants and interviewees were told to introduce themselves before speaking. This served as the basis for coding and sub-categorisation of the transcript.

6 FINDINGS

The workshop generated a significant amount of research data and for the purposes of this paper; a subset of the data is presented so as to maintain narrative coherence (Mcadams, 2006). Thus, this paper mainly presents a reconstructed subset of the research themes that were explored during the discussions and the interviews (Whitley and Kanellopoulou, 2010). The participants' accounts of their experiences and impressions clustered around the following key thematic areas: Empowerment, system quality, institutional cooperation, and the quality of service and information quality.

Participants were offered the opportunity to share their knowledge and impressions of identity management in general or a particular credential. A lack of user involvement or awareness usually affects the opinions and perceptions of a system (Davis, 1989). Examples of statements included: *"I do not know how the biometric based voter identity card will be verified"; "if I lose my national identity card I am not sure how and who to report to and how I can get another card"; "I do not know what the National Identity authority is trying to achieve. For instance how is it different from my voter ID card or my driving license? Do I have carry the card or I can only mention the card number and get served"*. These are all legitimate com-

ments that clearly show a lack of awareness and public education. Hence statements of this nature were categorised under user empowerment (Wilkinson, 1998).

Statements suggesting ease of use and usefulness, the experience of the credential issuers and the reliability of the system were all grouped under the common heading "system quality". Typical comments here included: *"I think biometric based voter identity cards can help weed out ghost names on the electoral register"*; *"I think with a biometric based voting systems the issue of long queues just to vote will be a thing of the past"*; *"I think national ID will make it easy to prove your citizenship or resident status since all must have one"*. These were expressions that indicate a perception of ease of use. However, many of the statements in this regards portrayed lack of reliability of the system. For instance: "*Prompt verification of my credential require Internet or mobile connectivity, how is this going to be possible given that in my village there is no Internet connection and the mobile connectivity is very poor"*; "*the technology used to store information on the NID card is a two dimensional barcode and so it will be difficult to store additional information on the card for secondary use purposes*". Obviously this shows that for a system to be of certain quality it is not just a question of the perceived usefulness and ease of use but also the reliability of the system is also very critical.
Trust in institutions emerged as vital element for adoption and usage of any government initiatives. As one of the respondents remarked:

"If the systems were to be run by qualified personnel, identity abuses like forged passports and driving licenses will be minimised. The appointment of many of the key decision makers in these organisations are based on factors other than qualification and experience. We only use it because we have no option for alternative".

Such statements clearly show a lack of trust in the institutions which issue credentials due to the perception that personnel handling the credentials are unqualified and inefficient. Trust in the institutions is also dependent on previous experiences with policy enforcement as recounted by another respondent;

"My brother sent me to withdraw foreign currency remittance from abroad, when I got to the bank the following day, I was told I had already collected the money. When I insisted that I had not been to the bank, I was shown a voter identity card bearing my name except the picture was different. I was advised to go the electoral commission for redress instead. It turned out that the other card was forged and the bank had no means of verifying. So at the moment I do not trust the voter's ID card or any other credential for that matter since they can easily be forged". This obviously implies lack of confidence in identity service providers.

We also noted from the discussions that one source of the distrust is as a result of lack of interoperability as chided by a participant; *"Why can't I present my drivers' license as proof of identity for voting in an election, if I misplace my voter ID card and why can't I present my voter ID as proof of qualification to drive if the police stops me whilst driving?. They all bear my name and other details"*.

A key reason for the lack of trust is the unreliability of important source documents like the birth certificate. This assertion is consistent to a statement made by a participant with national security background; "*if I am in doubt of the validity of the source document or can't verify its authenticity, why would I want to accept a secondary source as evidence"*.

Lack of citizens' trust in IdMS technology also play important role in trusted identities ecosystems, especially in relation to payment systems (Teo, et al., 2008). This is in relation to a remark by an interviewee with regard to the e-zwich[32] biometric based payment system in Ghana: *"I have confidence in agencies of the Bank of Ghana, but I think there is something wrong with the e-zwich technology – how can I make ATM withdrawal using my fingerprint details in a world where many of the available ATM's are not biometric based?"* Another stated *"assuming I transfer money to my parents in the village, how will they withdraw or receive the money when there is no e-zwich terminal in the area, and it will cost them about a third of the money sent in transport to go and withdraw the money in the district capital where there is no internet connection and the cell phone network is nothing to write home about?"* Such comments are indicative of a perceived lack of trust in the technology even when the agencies issuing the credentials are trustworthy.

The security aspect of the IdMS technology has also contributed to a lack of trust in the technology even where credential issuers are trusted institutions. For instance a major issue that resulted in a long debate and citizen's' apprehension towards the biometric based voter identity card system was when it became apparent that there would be no verification of identity. This raised the issue that "*if there will be no electronic verification card systems then what is the point of enrolling citizens into a card that cannot be verified"*, as remarked by a social commentator.

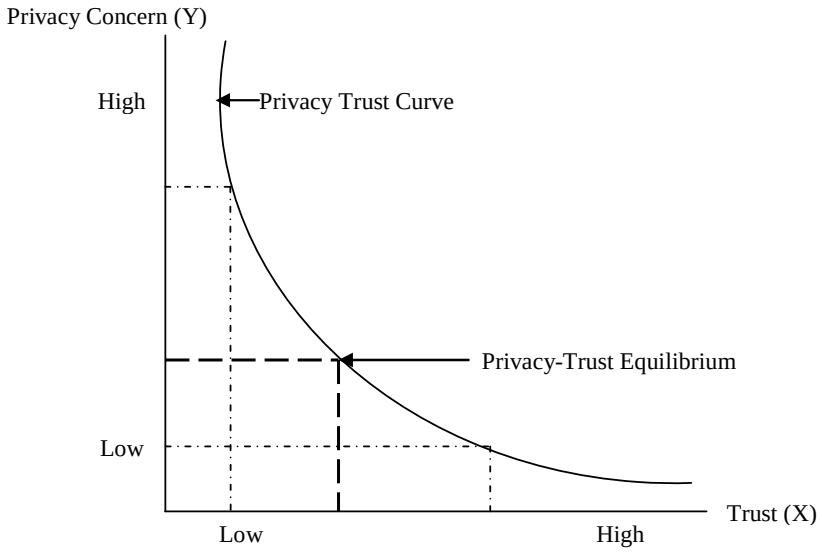
[32] e-zwich (GNA, 2012) is a biometric-based payment systems in Ghana that was aimed at making citizens adopt card based payments and also to offer a platform for the unbanked and less banked to be part of the banking system. The system is still operating but has since not been able to take-off as expected.

A factor that can inculcate citizens' confidence in IdMS technology is cyber and privacy laws and their enforcement. For instance in Ghana, privacy protection act was only passed into law on the 18th of May 2012, which obviously implies that prior to that, there was no specific information privacy law. Citizens' trust in IdMS technology will be enhanced if measures are taken to create awareness and public education about the system. This claim is in line with the following comments by interviewees; *"we have no idea how identity verification will be done on the Election Day, think the electoral commission should tell us how they will go about it"*. "*If I do not know how they are going to verify my identity how can I trust such a system*". Another participant's comment was even clearer that participants had no clue as to what is going on. *"How can laminated voter identity card store biometric details, are they going to use the number on the card to verify or what?"* This clearly shows that in implementing the biometric voter identification systems the implementing agency failed to adequately educate the public.

6.1 Privacy Concern -Trust Curve (PCTC)

The above analysis of the trust framework implies that society begins from a position of high privacy concern and thus distrust in identity management systems and service providers. As society begins to be more involved and understand the systems and there is more regulatory and technological interoperability, users are able to exercise some control over the presentation, authentication and verification of claims and credentials. Society becomes more empowered and also changes its negative perceptions about the institutions. This reduces the initial privacy concerns and increases trust. By implication a high privacy concern is associated with a low level of trust, and reduction in privacy concern can lead to an increase in trust. This relationship is represented in the privacy concern-trust curve in Figure III. The figure also depicts that absolute trust with zero privacy concerns might not be possible within a trusted identities framework and that is why the curve becomes asymptotic the closer we move to the further extremes of the curve. The purpose of the trust framework therefore is for society to work towards what we call *privacy concern–trust equilibrium.* The privacy concern–trust equilibrium is the point where trust and privacy is adequate enough to encourage more collaboration, creation of new identity based services, etc.

FIGURE III
PRIVACY CONCERN-TRUST CURVE (PCTC)



7 CONCLUSION

This study has shown that to ensure trusted identities, each stakeholder must be able to authenticate and verify identities on common terms and understanding. Undoubtedly, it is not enough to focus on system quality but also institutional corporation and collaboration with respect to interoperable technology, legal framework and standards on the supply side. On the demand side, there is the need for user empowerment which will result in informational self-determination in addition to service and information quality. The study also makes a profound contribution to the trusted identities literature by introducing what we have termed as privacy concern–trust curvilinear model for measuring the point of equilibrium between privacy concern and trust. The study has also shown that any attempt to ensure institutional cooperation and collaboration have the effect of enriching the trust within the identities ecosystem. In effect, through a collaborative effort and societal empowerment it is possible to realise trusted identities, which have the effect of pushing the relationship between trust and privacy concern towards equilibrium. It is at this equilibrium where majority of the benefits of trusted identities ecosystems can be realised.

It is however important to test empirically how realistic this is and whether the relationship between privacy concern and trust is a straight-line or curvilinear. Since our preliminary evaluation of the trusted identities framework was based on qualitative analysis, it will be interesting to evaluate the causality as noted in the trust framework quantitatively.

References

Adjei, J. K. and Olesen, H., (2011), "Keeping identity private, Vehicular Technology Magazine, IEEE, Vol. 6 No. 3, pp. 70-79.

Bélanger, F. and Crossler, R. E. (2011), "Privacy in the digital age: a review of information privacy research in information systems", MIS Quarterly, Vol. 35 No. 4, pp. 1017-1041.

Biskup, J. and Brüggemann, H. H., (1988), "The personal model of data: towards a privacy-oriented information system", Computers & Security, Vol. 7, pp. 575-597.

Bradwell, P., (2010), Private lives; a people's inquiry into personal information, Demos, London.

Burton-Jones, A. and Straub, D. W. J., (2006), "Reconceptualizing system usage: an approach and empirical test", Information Systems Research, Vol. 17 No. 3, pp. 228–246.

Clarke, R., (1994), "Human identification in information systems: management challenges and public policy issues", Information Technology and People, Vol. 7, pp. 6-37.

Cofta, P., (2008), "Towards a better citizen identification system", Identity in the Information Society, Vol. 1 No. 1, pp. 39-53.

Creswell, J. W., (2007), Qualitative Inquiry and Research Design: Choosing Among Five Approaches, Sage Publications, Thousand Oaks, CA.

Crosby, S. J., (2008), Challenges and Opportunities in Identity Assurance, http://www.hm-treasury.gov.uk/media/6/7/identity_assurance060308.pdf

Culnan, M. J., (1993), "'How did they get my name?': an exploratory investigation of consumer attitudes toward secondary information use", MIS Quarterly, Vol. 17 No. 3, pp. 341-363.

Davis, F. D., (1989), "Perceived usefulness, perceived ease of use, and user acceptance of information technology", MIS Quarterly, Vol. 13 No. 3, pp. 319-340.

Deci, E., Connell, J. and Ryan, R., (1989), "Self-determination in a work organization", Journal of Applied Psychology, Vol. 74 No. 4, pp. 580-590.

DeLone, W. H. and McLean, E. R., (2003), "The DeLone and McLean model of information systems success: a ten-year update", Journal of Management Information Systems,Vol. 19 No. 4, p. 9–30.

DeLone, W. and McLean, E., (1992), "Information systems success: the quest for the dependent variable", Information Systems Research, Vol. 3 No. 1, p. 60–95.

Dinev, T. and Paul, H., (2006), "Privacy concerns and levels of information exchange: an empirical investigation of intended e-services use", e-Service Journal, Vol. 4 No. 3, pp. 25-60.

EnCoRe, (2012), Ensuring Consent and Revocation (EnCoRe), http://www.encore-project.info

[Accessed 5 June 2012].

Farrell, H. and Knight, J., (2003), "Trust, institutions, and institutional change: industrial districts and the social capital hypothesis", Politics & Society, Vol. 31, pp. 537-566.

FIDIS, (2009), Trust and Identification in the Light of Virtual Persons, D17.4, WP 17, http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables/fidis-wp17-del17.4_Trust_and_Identification_in_the_Light_of_Virtual_Persons.pdf.

Gambetta, D. G., (1988), "Can we trust trust?", in Trust, Basil Blackwell, New York, pp. 213-237.

Giffin, K., (1967), "The contribution of studies of source credibility to a theory of interpersonal trust in the communication department", Psychological Bulletin, Vol. 68, pp. 104-120.

GNA, (2012), "Some controller staff apprehensive over use of e-zwich but...", http://www.modernghana.com/news/375344/1/some-controller-staff-apprehensive-over-use-of-e-z.html [Accessed 31 January 2012].

Grant, J. A., 2011. The National Strategy for Trusted Identities in Cyberspace Enhancing Online Choice, Efficiency, The National Strategy for Trusted Identities in Cyberspace Enhancing Online Choice, Efficiency, Security, and Privacy through Standards. IEEE Internet Computing, pp. 80-84.

Hardin, R., 1993. The Street-Level Epistemology of Trust. Politics & Society, 21(4), pp. 505-529.

IBM_Research, 2010. IDEMIX (Identity mixing) Project Overview. [Online]

Available at: http://www.zurich.ibm.com/pri/projects/idemix.html

[Accessed 28th February 2012].

Johnson-George, C. and Swap, W., (1982), "Measurement of specific interpersonal trust: construction and validation of a scale to assess trust in a specific other", Journal of Personality and Social Psychology, Vol. 43, pp. 1306-1317.

Jos, P. H., (2006), "Social contract theory: implications for professional ethics", The American Review of Public Administration, Vol. 36, pp. 139-155.

Kramer, R. M., (1999), "Trust and distrust in organizations: emerging perspective, enduring questions", Annual Review of Psychology, Vol. 50, pp. 569-598.

Lawler, E., (1992), The Ultimate Advantage: Creating the High-involvement Organization, Jossey-Bass, San Francisco.

Mayer, R. C., Davis, J. H. and Schoorman, D. F., 1995. An Integrative Model of Organizational Trust. The Academy of Management Review, July, 20(3), pp. 709-734.

Mcadams, D. P., (2006), "The problem of narrative coherence", Journal of Constructivist Psychology, Vol. 19 No. 2, pp. 109-125.

Microsoft_Connect, (2010), Microsoft U-Prove Community Technology Preview R2, https://connect.microsoft.com/site1188

Milberg, S. J., Smith, H. J. and Burke, S. J., (2000), "Information privacy: corporate management and national regulation", Organization Science, Vol. 11 No. 1, pp. 35-57.

Milne, G. R. G. M. E., (1993), "Direct mail privacy-efficiency trade-offs within an implied social contract framework", Journal of Public Policy & Marketing, Vol. 12 No. 2, pp. 206-215.

NSTIC, (2011), National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy, The White House, Washington DC.

O'Brien, J. A. and Marakas, G. M., (2010), Management Information Systems, McGraw Hill, Boston.

OECD, (2009), The Role of Digital Identity Management in the Internet Economy: a Primer for Policy Makers, http://www.oecd.org/dataoecd/55/48/43091476.pdf

OECD, (2011), Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy - Guidance for Government Policy Makers, http://dx.doi.org/10.1787/5kg1zqsm3pns-en

Pavlou, P. A., (2011), "State of the information privacy literature: where are we now and whee should we go?", MIS Quarterly, Vol. 35 No. 4, pp. 977-988.

Pavlou, P. A., Liang, H. and Xue, Y., (2007), "Understanding and mitigating uncertainty in online exchange relationships: a principal–agent perspective", MIS Quarterly, Vol. 31(No. 1, pp. 105-136.

Petter, S., DeLone, W. and McLean, E., (2008), "Measuring information systems success: models, dimensions, measures, and interrelationships", European Journal of Information Systems, Vol. 17, pp. 236-263.

Raab, C. D., (2005), "The future of privacy protection", in Trust and Crime in Information Societies, Edward Elgar, Cheltenham, pp. 282-318.

Regan, P. M., (2002), "Privacy as a common good in the digital world", Information, Communication & Society, Vol. 5 No. 3, pp. 382-405.

Rosen, B. and Jerdee, T. H., (1977), "Influence of subordinate characteristics on trust and use of participative decision strategies in a management simulation", Journal of Applied Psychology, Vol. 62, pp. 628-631.

Schaupp, L. C., Fan, W. and Belanger, F., (2006), "Determining success for different website goals", in the Proceedings of the 39th Hawaii International Conference on System Sciences (HICSS), Kauai, Hawaii, pp. 1-10.

Smith, J. A., (2004), "Reflecting on the development of interpretative phenomenological analysis and its contribution to qualitative research in psychology", Qualitative Research in Psychology, Vol. 1 No. 1, pp. 39-54.

Smith, R., (2004), "A matter of trust : service users and researchers', Qualitative Social Work, Vol. 3 No. 3, pp. 335-346.

Stone, E. F., Gardner, D. G., Gueutal, H. G. and McClure, S., (1983), "A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations", Journal of Applied Psychology, Vol. 68 No. 3, pp. 459-468.

Teo, T. S., Srivastava, S. C. and Jian, L., (2008), "Trust and electronic government success: an empirical study", Journal of Management Information Systems, Vol. 25 No. 3, p. 99–131.

Tolchinsky, P. D. et al., (1981), "Employee perceptions of invasion of privacy: a field simulation experiment", Journal of Applied Psychology, Vol. 66 No 3, pp. 308-313.

Trubow, G., (1992), "Personal privacy and secondary-use dilemma (social aspects of automation)", Software, IEEE, Vol. 9 No. 4, pp. 73-74.

Urbach, N. and Müller, B., (2012), "The updated DeLone and McLean model of information systems success, in Information Systems Theory: Explaining and Predicting, Springer, pp. 1-18.

Whitley, E. A. and Kanellopoulou, N., (2010), "Privacy and informed consent in online interactions: evidence from expert focus groups", International Conference on Information Systems, St Louis.

WHO, (2012), World Health Statics 2012,
http://www.who.int/gho/publications/world_health_statistics/2012/en/

Wilkinson, A., (1998), "Empowerment: theory and practice", Personnel Review, Vol. 27 No. 1, pp. 40-56.

Wilson, J. Q., (1989), Bureaucracy: What Government Agencies Do and Why They Do It, Basic Books, NewYork.

Wilton, R., (2008), "Identity and privacy in the digital age", International Journal of Intellectual Property Management, Vol. 2 No. 4, p. 411 428.

Yin, R. K., (2011), Qualitative Research from Start to Finish, The Guilford Press, New York.

Appendices

Stakeholder Workshop Invitation Letters and Programs

GHANA TELECOM UNIVERSITY COLLEGE

January 9, 2012

Dear Sir/Madam,

INVITATION TO STAKEHOLDER WORKSHOP

Ghana Telecom University College in conjunction with Aalborg University, Denmark, is pleased to invite you to a one day stakeholder's workshop on the theme **"Secondary Use and Commercialization of Personal Information: Technology, Policies and Regulatory Framework"**. The details are as follows:

Date: Monday 16th January, 2012
Time: 9:00am – 12:00pm
Venue: Video Conference Centre, Ghana Telecom University College, Tesano Campus

Secondary uses of personal information have become necessary in various jurisdictions because majority of business and social interactions entails various forms of identity verifications and identity assurances. This undoubtedly implies that secondary use of personal information can promote or facilitate effective public services, business activities, and new business opportunities. Incidentally, this personal information usage also presents complex ethical, technological and social challenges, which usually borders on privacy, trust and security. Such negative side effects have played significant role in impeding access to and the expansion of secondary use of personal information.

In Ghana, several independent Identity Management (IDM) initiatives are under way. This includes National Identity Card System, National Health Insurance Scheme, Biometric Passport, Biometric Drivers' Licence, Biometric Voters' Identity Cards, etc. It is however not clear what steps businesses go through in order to take advantage of such information for secondary and commercial uses. Moreover, many of the ID projects in Ghana have focus on physical verification with little emphasis on online or internet based authentications.

The objective of the workshop is to bring key stakeholders together and to identify the major policy, technological, regulatory and commercial issues involved in the use of personal information. The program will take the form of plenary and roundtable discussions during which invited participants will be given the opportunity to ask questions and address the issues from their perspective.

The outcome of the workshop will help research work in Identity Management and Commercial uses of Personal Information. Your input is therefore critical to the success of the workshop.

We look forward to welcoming you.

Yours sincerely,

Dr. Robert Awuah Baffour
Vice President, GTUC

Private Mail Bag 100, Accra North. Tel: 030-2221402 /222146 /2221456 /2221479 / Fax:030-2223531
E-mail: info@gtuc.edu.gh Website: http://www.gtuc.edu.gh

November 6, 2012

The Head of IT

Central University College

Accra

Dear Sir,

INVITATION TO STAKEHOLDER WORKSHOP

Ghana Technology University College (GTUC) in conjunction with Aalborg University, Denmark, is pleased to invite you to a one day stakeholder's workshop on the theme "Best Practices in Crafting Trusted Identity Management Systems". This is a follow-up on a previous workshop in January which addressed the technological, regulatory and policy implications on secondary uses and commercialisation of personal identity information. The details are as follows:

Date: Tuesday 6th November, 2012

Time: 9:00am – 4:00pm

Venue: Ghana Telecom University College, Tesano Campus

Governments in many countries have implemented some form of identity management systems as a critical enabler of government to citizens' interactions, and in facilitation of sensitive transactions and activities like elections, cross-border control, online banking, accessing electronic health records, etc. Unfortunately, there is the tendency to equate identity credentials to "identity of a person" resulting in the issue of various forms of credentials to citizens for specific purposes. Many of the Identity credentials focus on physical verification with little emphasis on digital and Internet-based authentication, which reduces the expected improvement in public services and societal interactions.

The objective of the workshop is to bring key stakeholders together to identify the major issues involved in crafting trusted identities that can help in removing the barriers that preclude key stakeholders from easily adopting digital identification technologies that are secure and trusted and for commercial purposes.

The program will take the form of plenary sessions during which invited participants will be given the opportunity to ask questions and address issues from their perspective. This will be followed by focus group discussions. The outcome of the workshop will help policy formulation and research work in trusted identity management and Commercial uses of Personal Information. Your input is therefore critical to the success of the workshop.

We look forward to welcoming you.

Yours Sincerely,

DR. GILBERT ARYEE

DIRECTOR OF RESEARCH, GTUC

GHANA TECHNOLOGY UNIVERSITY COLLEGE

PROGRAM- RESEARCH SEMINAR

Date: Tuesday, 6th November, 2012
Time: 9:00am – 3:00pm
Venue: Eva Von Hirsch Auditorium

Theme: Best Practices in Implementation of Trusted Identity Management Systems

9:00am – 9:15am	Arrival and Registration
9:15am – 9:20am	Opening Prayer
9:20am – 9:30am	Opening Remarks Dr. Gilbert Aryee, Director of Research, GTUC
9:30am – 9:40am	Remarks National Identification Authority Dr. William Ahadzie, Executive Secretary, NIA
9:40am – 9:50am	Remarks by The Electoral Commission
9:50am – 10:05am	Keynote Address Dr. Robert Awuah Baffour, President, GTUC
10:05am – 10:20am	Group Picture and Snack Break
10:20am – 10:40am	Presentation Joseph Kwame Adjei, PhD Fellow, CMI, Aalborg
10:40am – 10:50am	Q & A
10:50am – 11:10am	Presentation Registrar, Birth & Death Registry
11:10am – 11:30am	Presentation, Victoria Boateng, National ICT Authority (NITA)
11:30am – 11:50am	Presentation Mr. Thomas Baafi, CEO, B-Systems
11:50am – 12:30pm	Question and Answer Session
12:30pm – 1:30pm	Lunch
1:30pm – 2:30pm	Group Discussion
2:30pm – 3:00pm	Group Presentation
3:00pm – 3:05pm	Closing Remarks, Dr. Gilbert Aryee, Director of Research, GTUC
3:05pm	Closing Prayer

SAMPLE LIST OF SECOND WORKSHOP PARTICIPANTS

NAME	ORGANIZATION	TEL NO	EMAIL ADDRESS
Enock Kyei	Ministry Of Foreign Affairs	0277602112	enokyei@yahoo.com
Kweku William Halm	Registrar General's Department	0202728931	kwekuhalm@yahoo.com
Divine Akuoko	Dataspace Consulting	0243104021	divine.barrack@gmail.com
Mawutodzi Abissath	Information Service Department	0244773085	abissath@gmail.com
Frank Kwasi Asante	Information Service Department	0277406979	asante_fk@hotmail.com
E. L. Asiedu	Ghana Post	0244995261	elasiedu@yahoo.com
Gilbert Aryee	Ghana Telecom University College	0202698320	garyee@GTUC.edu.gh
Henry Myers-Aboagye	National Identification Authorit Y	0208135079	hmaboagye@gmail.com
Joana Nyarko-Mensah	Ministry Of Foreign Affairs	0261174036	maameafrifa@yahoo.com
Salim Ibrahim	Ministry Of Foreign Affairs	0242859565	salinkoex@gmail.com
Godson Lazekpo	Ssnit	0202015486	gladzekpo@SSNIT.org.g
Danny Hammond	Ministry Of Defence	0242958000	dnahammond@gmod.gove.gh
Amevor Prince Albert	Ministry Of Defence	0244012492	princeogy@yahoo.com
Kwame Ofosu Obeng	Ghana Institute Of Jounalism	0244749885	obeng_ofosu@yahoo.com
Goerge Tudzi	MWRWH	0208192249	evangelsys@yahoo.com
Alex Q. Papafio	Ecobank	0261128722	alqp7@gmail.com
Magmus Awuah	Ghana Revenue Authority	0243346776	magmus.awuah@gra.gov.gh
Dennis Okyere	Bsystems Ltd	0247235291	dennis@bsystemslimited.com
Victor A. Sackey	Mofa Passport Office Ridge	0243571052	vaswoa@yahoo.com
Kingsley A. Addo	Birth & Death	0244215830	kingaddo@yahoo.com
Seth Bosompem Kissi		0244642817	swagahs@gmail.com
Veronica Boateng	NITA	0202050187	veronica.boateng@nita.gov.gh

NAME	ORGANIZATION	TEL NO	EMAIL ADDRESS
Tweneboah Koduah	GIMPA	0245349741	stkoduah@gimpa.edu.gh
Kevin Philip Quansah	Bsystems	0244857028	kevinquansah@gmail.com
Salomey Braimah	Births & Deaths	0208257824	braimah_s@ymail.com
Andy Fosu	Ghana News Agency	0244293247	
Comfort Fetrie	Ghana News Agency	0244293247	
J. Gambo	M.E.R.Taz	-	koranza@gmail.com
Sebasting A. Yevugah	Ministry Of Foreign Affairs	0244284300	syevugah@yahoo.com
Veronica Adjei	Brookes Institute	0276634162	ronikay25@hotmail.com
Participant	Electoral Commission		
Francis Akwasi-Kuma	Ghana Revenue Authority	0244262111	fkuma@gra.gov.gh
Kwasi Aboagye	Ministry of Lands And Natural Res.	0208628730	kwasiaboagye1988@yahoo.com
Frank Oye	Margins Group	0200721293	frankoye@googlemail.com
Joseph Tetteh	Ministry of Communication	0208161609	joseph.tetteh@moc.gov.gh
Emmanuel Fiagbenu	Ghana Multimedia Inc. (Gmic)	0244289856	e.fiagbenu@yahoo.com
Daniel Mohammed	Data Link University	0244569211	danblow000@yahoo.com
Dorgbetor Solomon	Data Link University	0208259154	sdorgbetor@gmail.com
Emmanuel N. Botchway	Births & Deaths	0244161894	emmabotchway@yahoo.co.uk
F. Agyenim	GTUC	0202698369	kingaddo@yahoo.com
Nancy Essien	NCCE	0244998873	swagahs@gmail.com
Cephas Adjei Mensah	MOE	0244888566	veronica.boateng@nita.gov.gh
Tweneboah Kodua	GIMPA	0244667590	stkoduah@gimpa.edu.gh
Farouk	CIO, Ghana Commercial Bank		
Reporter	Ghana News Agency		
Reporter	Ghana News Agency		